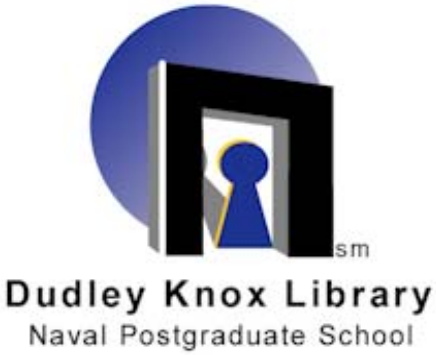
2008-01

Information Warfare and Information Operations (IW/IO) : A Bibliography

Marlatt, Greta E.

INFORMATION WARFARE AND INFORMATION OPERATIONS (IW/IO): A BIBLIOGRAPHY



Compiled by

Greta E. Marlatt
Dudley Knox Library
Naval Postgraduate School
Revised and updated
January 2008

This Bibliography is also available at
http://www.nps.edu/Library/Research/Bibliographies/index.html

INFORMATION WARFARE and INFORMATION OPERATIONS (IW/IO): A BIBLIOGRAPHY

Complied by

Greta E. Marlatt

Dudley Knox Library
Naval Postgraduate School
Revised and Updated
January 2008

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Definitions

Cyber Warfare (CyW) [1]
Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system. CyW includes the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid.

Information Assurance [2]
(DOD) Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Operations [2]
(DOD) Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Superiority [2]
(DOD) The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. NOW CHANGED TO That degree of dominance in the information domain which permits the conduct of operations without effective opposition.

Information Warfare [2]
(DOD) Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW. [4] Information Warfare is any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions

Network Centric Operations [3]
Network Centric Operations (NCO) involves the development and employment of mission capability packages that are the embodiment of the tenets of **Network Centric Warfare (NCW)** in operations across the full mission spectrum. These tenets state that a robustly networked force improves information sharing and collaboration, which enhances the quality of information, the quality of awareness, and improves shared situational awareness. This results in enhanced collaboration and enables self-synchronization improving sustainability and increasing the speed of command, which ultimately result in dramatically increased mission effectiveness.

Psychological Operations [2]
(DOD) Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of

psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP.

Psychological Warfare [2]
(DOD) The planned use of propaganda and other psychological actions having the primary purpose of influencing the opinions, emotions, attitudes, and behavior of hostile foreign groups in such a way as to support the achievement of national objectives. Also called PSYWAR. See also psychological warfare consolidation. [this definition has now been removed from the DoD Dictionary]

*[1] from **DoD Dictionary** -- http://www.dtic.mil/doctrine/jel/doddict/*

*[2] from Alford, Lionel D., Jr. "Cyber Attack: Protecting Military Systems." **Acquisition Review Quarterly**, Spring 2000, v. 7, no. 2, p. 105.*
http://www.dau.mil/pubs/arq/2000arq/alford.pdf

*[3] from **Military Operations Research Society [MORS]***
http://www.mors.org/meetings/oa_nco/oa_definition.htm

*[4] from Borden, Andrew. "What is Information Warfare?" **Chronicles Online Journal**, November 1999.*
http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html

Information Warfare

Books

Adams, James. **The Next World War: Computers are the Weapons and the Front Line is Everywhere**. New York: Simon & Schuster, c1998. 366p.
DKL U163 .A33 1998 GENERAL

Adkins, Bonnie N. **The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?** Maxwell AFB, AL: Air University, Air Command and Staff College, 2001. 37p.
https://research.maxwell.af.mil/viewabstract.aspx?id=3610

Air Land Sea Applications Center. **Information Warfare/Information Operations Study**. Staff Study, 15 December 1995.

Alberts, David S. **Defensive Information Warfare**. Washington, DC: National Defense University, [1996] 80p.
DKL D 5.402:D 36/4 FEDDOCS
http://www.dodccrp.org/files/Alberts_Defensive.pdf

_____. **Power to the Edge: Command and Control in the Information Age.** Washington, DC: Command and Control Research Program, National Defense University, 2003. 259p.
http://www.dodccrp.org/files/Alberts_Power.pdf
DKL UB212 .A43 2003 GENERAL

_____. **The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative**. Washington, DC: National Defense University, Institute for National Strategic Studies, 1996. 62p.
DKL UG485 .A42 1996 GENERAL
http://www.ndu.edu/inss/books/books%20-%201996/Unintended%20Consequences%20-%20April%2096/uchome.html

Alberts, David S., et al. **Understanding Information Age Warfare**. Washington, DC: CCRP Publication Series, 2001. 312p.
DKL U 163 .U49 2001 GENERAL
http://www.dodccrp.org/files/Alberts_UIAW.pdf

Alberts, David S. and Daniel S. Papp. **The Information Age: An Anthology on Its Impact and Consequences**. Washington, DC: National Defense University, Institute for National Strategic Studies, 1997. Vols. 1-4.
DKL T58.5 .I5224 1997 v. 1-4 GENERAL
http://www.ndu.edu/inss/books/books%20-%201998/Information%20Age%20Anthology%20-%20Sept%2098/index.html

Alberts, David S. and Richard E. Hayes. “Information Warfare Workshop: Decision Support Working Group Report.” p. 569-576, IN: **Proceedings of the First International Symposium on Command and Control Research and Technology.** Washington, DC: National Defense University, 19-22 June 1995. Washington, DC: National Defense University, 1996. 600p.
DKL UB212 .I573 1995 GENERAL

Allard, C. Kenneth. **Command, Control and the Common Defense**. New Haven: Yale University Press, 1990. 317p.
DKL UA23 .A593 1990 GENERAL

Allard, C. Kenneth. **Command, Control and the Common Defense**. Rev. ed. Washington, DC: National Defense University, 1996. 359p.
DKL UA23 .A593 1996 GENERAL
http://www.ndu.edu/inss/books/Books%20-%201996/Command%20Control%20and%20Common%20Def%20-%20Oct%2096/CCCD.pdf

Anderson, Robert H., et al. **Securing the U.S. Defense Information Infrastructure: A Proposed Approach**. Santa Monica, CA: Rand, 1999. 158p.
DKL UB247 .S425 1999 GENERAL
http://www.rand.org/pubs/monograph_reports/MR993/index.html

Armistead, Leigh. (Ed.). **Information Warfare: Separating Hype from Reality.** Washington, DC: Potomac Books, Inc., c2007. 189p.
Contents: Introduction: "Brother, can you spare me a DIME?" -- Dan Kuehl, senior IO instructor, National Defense University -- Updates to IO policy and organizations -- Leigh Armistead, Edith Cowan University and strategic IA manager, Honeywell – Perception management: IO's stepchild -- Pascale Siegel,
president, Insight through Analysis – Information operations in the global war on terror: lessons learned from operations in Afghanistan and Iraq -- Zachary P. Hubbard, former IO division head, JFSC and senior manager, MTSTech -- Cyberterrorism: hype and reality -- Maura Conway, lecturer, Dublin City University -- Information operations education: lessons learned from information assurance – Corey Schoum director, NIATEC -- Dan Kuehl, Leigh Armistead -- Information operations and the average citizen -- David Wolfe, chief operations officer, IA, directorate, Honeywell -- A tale of two cities: approaches to counter-terrorism and critical infrastructure protection in Washington, D.C. and Canberra -- Jeffrey Malone, IO analyst, Noetic Solutions Pty Ltd., Leigh Armistead -- Speaking out of both sides of your mouth: perception management approaches in Washington, D.C. and Canberra – Jeffrey Malone, Leigh Armistead -- Conclusion – Leigh Armistead.
DKL U163 .I543 2007 GENERAL

Arquilla, John. “Ethics and Information Warfare.” p. 379-401, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
DKL UG478 .C43 1999 GENERAL
http://www.rand.org/pubs/monograph_reports/MR1016/index.html

Arquilla, John and David Ronfeldt. **Emergence of Noopolitik Toward an American Information Strategy**. Santa Monica, CA: Rand, 1999. 99p.
DKL JZ1254 .A77 1999 GENERAL
http://www.rand.org/pubs/monograph_reports/MR1033/index.html

_____. **In Athena's Camp: Preparing for Conflict in the Information Age**. Santa Monica, CA: Rand, 1997. 501p.
DKL U21.2 .A74 1997 GENERAL
http://www.rand.org/pubs/monograph_reports/MR880/index.html

Arquilla, John and Douglas A. Borer (eds.). **Information Strategy and Warfare: A Guide to Theory and Practice**. New York: Routledge, 2007. 248p.
DKL U163 .I54 2007 GENERAL

Ayres, Richard R., et al. **Information Warfare: Planning the Campaign**. Maxwell AFB, AL: Air University, Air Command and Staff College, 1996. 68p.
http://handle.dtic.mil/100.2/ADA331946

Barnett, Jeffrey R. **Future War: An Assessment of Aerospace Campaigns in 2010**. Maxwell Air Force Base, AL: Air University Press, January 1996. 169p.
http://aupress.maxwell.af.mil/Books/b-5/b5.htm

Bennett, Bruce W., Christopher Twomey and Gregory F. Treverton. **What are Asymmetric Strategies?** Santa Monica, CA: Rand, 1999. 24p.
DKL U153 .B46 1999 GENERAL
http://www.rand.org/pubs/documented_briefings/2005/DB246.pdf

Bennett, Sheila G. **A Process for Vectoring Offensive Information Warfare as a Primary Weapon Option Within the United States Air Force**. Wright-Patterson AFB, OH: Air Force Institute of Technology, 2001. 150p.
https://research.maxwell.af.mil/viewabstract.aspx?id=2607

Bernhardt, Ute. "The Empire Strikes Back." p. 137-143, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Berry, James W. **The New Military Strategy: Command and Control Warfare**. Maxwell AFB, AL: Air University, Air War College, April 1996. 29p.

Black, Steven K. **Russia's Armed Forces on the Brink of Reform**. Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1998. 45p.
DKL UA770 .B8543 1998 GENERAL
http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=143

_____. **A Sobering Look at the Contours of Cyberspace**. Ridgway Viewpoints; No. 96-3. Pittsburgh, PA: Ridgway Center for International Security Studies, University of Pittsburgh, 1996. 73p.
DKL TK5105.5 .B52 1996 GENERAL

_____. **This Page Under Construction: Information Warfare in the Post-Cold War World**. Ridgway Viewpoints; No. 96-1. Pittsburgh, PA: Matthew B. Ridgway Center for International Security Studies, University of Pittsburgh, [1996]. 27p.
DKL U163 .B62 1996 GENERAL

Boacun, Wang and Li Fei. "Information Warfare." p. 327-342, IN: Pillsbury, Michael (ed.). **Chinese Views of Future Warfare**. Washington, DC: National Defense University Press, 1997. 421p.
DKL UA835 .C453 1997 GENERAL
http://www.fas.org/irp/world/china/docs/iw_wang.htm
http://www.au.af.mil/au/awc/awcgate/ndu/chinview/chinacont.html

Buchan, Glenn C. "Implications of Information Vulnerabilities for Military Operations." p. 283-323, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
DKL UG478 .C43 1999 GENERAL
http://www.rand.org/pubs/monograph_reports/MR1016/index.html

_____. **Information War and the Air Force: Wave of the Future? Current Fad?** Issue Paper. Santa Monica, CA: Rand, 1996. 14p.
http://www.rand.org/pubs/issue_papers/2006/IP149.pdf

Builder, Carl. "The American Military Experience in the Information Age." p. 19-44, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
DKL UG478 .C43 1999 GENERAL
http://www.rand.org/pubs/monograph_reports/MR1016/index.html

Butler, Bradley L. **The Need for a USAF Information Warfare (IW) Strategy for Military Operations Other Than War (MOOTW).** Maxwell AFB, AL: Air University, Air War College, April 1996. 43p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1493

Campen, A. D. (ed.). **The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War**. Fairfax, VA: AFCEA International Press, 1992. 195p.
DKL UB212 .F57 1992 GENERAL

Carlson, Adolph. "A Chapter Not Yet Written: Information Management and the Challenge of Battle Command." p. 103-124, IN: Neilson, Robert E. (ed.). **Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition**. Washington, DC: National Defense University Press, 1997. 167p.
DKL D 5.402:Su 7 FEDDOCS
http://www.ndu.edu/inss/siws/ch5.html

Corcoran, Michael J. and J. P. MacIntosh. "Military Operations and Their Reliance on the National Information Infrastructure (NII) and Minimum Essential Defense Information Infrastructure (MEDII) in an Information Warfare Scenario." p. 922-925, IN: **Proceedings of the 1998 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 29 June - 1 July 1998. Washington, DC: National Defense University, 1998. 943p.
DKL UB212 .C68 1998 GENERAL

Cordesman, Anthony H. **Defending America: Redefining the Conceptual Borders of Homeland Defense: Critical Infrastructure Protection and Information Warfare.** Washington, DC: Center for Strategic and International Studies, 2000.
http://www.csis.org/component/option,com_csis_pubs/task,view/id,1653/type,1/

Davis, Harry J. **Developing Air Force Information Warfare Operational Doctrine: The Crawl-Walk-Run Approach**. Maxwell AFB, AL: Air University, Air War College, April 1996. 34p.

Davis, Lynn E. "Arms Control, Export Regimes and Multilateral Cooperation." p. 361-377, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Definitions for the Discipline of Information Warfare. [Washington, DC]: National Defense University, School of Information Warfare and Strategy, [1996] 84p.
DKL U163 .D43 1996 GENERAL

Denning, Dorothy E. **Information Warfare and Security**. New York: ACM Press; Reading, MA: Addison-Wesley, c1999. 522p.
DKL U163 .D46 1999 GENERAL

Denning, Peter (ed.) **Computers Under Attack: Intruders, Worms, and Viruses.** New York: Addison-Wesley, 1990. 554p.
DKL QA76.9 .A25 C667 1990 GENERAL

Denno, Patricia, Gregory Drew and Aaron Temin. "Comprehensive Vulnerability Assessments for Defense Information Warfare." p. 559-576, IN: **Proceedings of the 1998 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 29 June - 1 July 1998. Washington, DC: National Defense University, 1998. 943p.
DKL UB212 .C68 1998 GENERAL

Devost, Matthew G. and Brian K. Houghton. "Information Terrorism: Can You Trust Your Toaster?" p. 63-78 IN: Neilson, Robert E. (ed.). **Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition**. Washington, DC: National Defense University Press, 1997. 167p.
http://www.ndu.edu/inss/siws/ch3.html
DKL D 5.402:Su 7 FEDDOCS

Dines, Robert. "CIS Survivability Assessment." p. 227-232, IN: **Proceedings of the Second International Symposium on Command and Control Research and Technology.** Market Bosworth, United Kingdom, 24-26 June 1996. Washington, DC: National Defense University, 1997. 592p.
DKL UB212 .I573 1997 GENERAL

Dockery, John. "Living With Viruses." p. 233-239, IN: **Proceedings of the Second International Symposium on Command and Control Research and Technology.** Market Bosworth, United Kingdom, 24-26 June 1996. Washington, DC: National Defense University, 1997. 592p.
DKL UB212 .I573 1996 GENERAL

Downs, Lawrence G., Jr. **Digital Data Warfare: Using Malicious Computer Code as a Weapon**. Maxwell Air Force Base, AL: Air War College, Air University, 1995. 33p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1623

_____. "Digital Data Warfare: Using Malicious Computer Code as a Weapon" p. 43-80, IN: Sommerville, Mary A. (ed.) **Essays on Strategy XIII**. Washington, DC: National Defense University Press, 1996. 333p.
DKL D 5.204:Es 7/3/1996 FEDDOCS

Druffel, Larry. "Defensive Information Warfare in the 21st Century." p. 17-31, IN: **Information Applications Volume, New World Vistas: Air and Space Power in the 21st Century.** [Washington, DC?: USAF Scientific Advisory Board, 1995-]
http://www.fas.org/spp/military/docops/usaf/vistas/vistas.htm
DKL D 301.118:P 87/2/INFORM FEDDOCS

Dunnigan, James F. **Digital Soldiers: The Evolution of High Tech Weaponry and Tomorrow's Brave New Battlefield**. New York: St. Martin's Press, 1996. 309p.
DKL UF500 .D87 1996 GENERAL

Erbschloe, Michael. **Information Warfare: How to Survive Cyber Attacks**. New York, NY: Osborne/McGraw-Hill, c2001. 315p.
DKL U163 .E66 2001 GENERAL

Everett, Charles B., et al. "The Silicon Spear: An Assessment of Information Based Warfare and U.S. National Security." p. 33-62, IN: Neilson, Robert E. (ed.). **Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition**. Washington, DC: National Defense University Press, 1997. 167p. *http://www.ndu.edu/inss/siws/ch2.html*
DKL D 5.402:Su 7 FEDDOCS

Fast, William R. "Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age." p. 3-32 IN: Neilson, Robert E. (ed.). **Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition**. Washington, DC: National Defense University Press, 1997. 167p. *http://www.ndu.edu/inss/siws/ch1.html*
DKL D 5.402:Su 7 FEDDOCS

Faurer, Lincoln D. "Offensive Information Warfare in the 21st Century." p. 66-71, IN: **Information Applications Volume, New World Vistas: Air and Space Power in the 21st Century.** [Washington, DC?: USAF Scientific Advisory Board, 1995-]
http://www.fas.org/spp/military/docops/usaf/vistas/vistas.htm
DKL D 301.118:P 87/2/INFORM FEDDOCS

FitzGerald Mary C. "Russian Views on Electronic and Information Warfare." p. 126-163, IN: **Proceedings of the Third International Symposium on Command and Control Research and Technology.** National Defense University, Washington, DC, 17-20 June 1997. Washington, DC: National Defense University, 1997. 893p.
DKL UB212 .I573 1997 GENERAL

Forno, Richard and Ronald Baklarz. **Art of Information Warfare: Insight Into the Knowledge Warrior Philosophy**. Universal Publishers, c1999. 180p.
DKL UG485 .F67 1999 GENERAL

Fox, Steven G. "Unintended Consequences of Joint Digitization." p. 125-144, IN: Neilson, Robert E. (ed.). **Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition**. Washington, DC: National Defense University Press, 1997. 167p.
http://www.ndu.edu/inss/siws/ch6.html
DKL D 5.402:Su 7 FEDDOCS

Fredericks, Brian. “Information Warfare: The Organizational Dimension.” p. 79-102, IN: Neilson, Robert E. (ed.). **Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition**. Washington, DC: National Defense University Press, 1997. 167p.
http://www.ndu.edu/inss/siws/ch4.html
DKL D 5.402:Su 7 FEDDOCS

Frye, Dwayne W. **Information Warfare (IW): Air Staff Roles and Responsibilities**. Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 39p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1124

Fukuyama, Francis and Abram N. Shulsky. “Military Organization in the Information Age: Lessons From the World of Business.” p. 327-360, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Furst, David A. **Information Warfare: Seriously!!** Maxwell AFB, AL: Air University, Air War College, April 1996. 34p.

Garian, Robert. **Information Warfare: Russia, France, and the United Kingdom**. Washington, DC: Federal Research Division, Library of Congress, 1995. 30p.
DKL I163 .G37 1995 GENERAL

Gauthier, Kathryn L. **China as Peer Competitor?: Trends in Nuclear Weapons, Space, and Information Warfare.** Maxwell Air Force Base, AL: Air War College, Air University, [1999]. 39p.

Geyer, Michael. "Electronic Ways of Death." p. 144-152, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Gillam, Mary M. **Information Warfare: Combating the Threat in the 21st Century**. Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 52p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1122

Gompert, David C. “Right Makes Might: Freedom and Power in the Information Age.” p. 45-73, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Gray, Chris Hables. "The Crisis of Info War." p. 130-136, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Grinter, Lawrence E. **The Dragon Awakes: China's Military Modernization Trends and Implications**. Maxwell, AFB, AL: Air University, USAF Counterproliferation Center, 1999. 94p.
DKL UA837 .D72 1999 GENERAL

Gruber, David J. **Computer Networks and Information Warfare: Implications for Military Operations.** Center for Strategy and Technology Occasional Paper No. 17. Maxwell Air Force Base, AL: Center for Strategy and Technology, Air War College, 2000. 29p.
Contents: 1. Introduction. -- II. Military operations and information systems. -- III. Emergence of networks. -- IV. Expeditionary Air Force and information networks. -- V. Framework for computer network defense. -- VI. Conclusion.
http://www.au.af.mil/au/awc/awcgate/cst/csat17.pdf
http://purl.access.gpo.gov/GPO/LPS46267
DKL D 301.26/6-A:17 FEDDOCS

Hall, Wayne Michael. **Stray Voltage: War in the Information Age**. Annapolis, MD: Naval Institute Press, 2003. 219p.
DKL UA23 .H34 2003 GENERAL

Harshberger, Edward and David Ochmanek. "Information and Warfare: New Opportunities for U.S. Military Forces." p. 157-178, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Hayes, Peter. "How Air Command is Responding to the Information Warfare Challenge." p. 37-47, IN: Brent, Keith (ed.). **Regional Air Power Workshop, Canberra, 23-25 September 1997**. Australia: Royal Australian Air Force, Air Power Studies Centre, 1997. 182p.

Henning, Paul R. **Air Force Information Warfare Doctrine: Valuable or Valueless?** Maxwell AFB, AL: Air University, Air Command and Staff College, March 1997. 39p.
http://www.au.af.mil/au/awc/awcgate/acsc/97-0604c.pdf

Henry, Ryan and Peartree, C. Edward, eds. **The Information Revolution and International Security**. (Significant issues series, v. 20, no. 1)
Washington, DC: CSIS Press, 1998. 194p.
DKL JZ5588 .I54 1998 GENERAL

Hundley, Richard O. and Robert H. Anderson. **A Qualitative Methodology for the Assessment of Cyberspace-Related Risks**. P-7988. Santa Monica, CA: Rand, 1996. 35p.
DKL TK5105.59 .H87 1996 GENERAL

Hurley, Patrick M. and Jerry L. Dussault. "The Development and Assessment of an Adaptive Fault Resistance System." p. 256-266, IN: **Proceedings of the Second International Symposium on Command and Control Research and Technology.** Market Bosworth, United Kingdom, 24-26 June 1996. Washington, DC: National Defense University, 1997. 592p.
DKL UB212 .I573 1996 GENERAL

Hutchinson, William and Matthew Warren. **Information Warfare: Corporate Attack and Defence in a Digital World.** Oxford: Butterworth-Heinemann, 2001. 208p.
DKL QA 76.A25 H87 2001 GENERAL

Janczewski, Lech and Andrew M. Colarik. **Managerial Guide for Handling Cyber-Terrorism and Information Warfare.** Hershey, PA: Idea Group Pub., 2005. 229p.
DKL HV 6773 .J354 2005 GENERAL

Jensen, Richard M. **Information War Power: Lessons from Air Power**. Cambridge, MA: Harvard University, Program on Information Resources Policy, Center for Information Policy Research, 1997. 82p.

Jincheng, Wei. "Information War: A New Form of People's War." p. 409-412, IN: Pillsbury, Michael (ed.). **Chinese Views of Future Warfare**. Washington, DC: National Defense University Press, 1997. 421p.
http://www.ndu.edu/inss/books/books%20-%201998/Chinese%20Views%20of%20Future%20Warfare%20-%20Sept%2098//chinacont.html
DKL UA835 .C453 1997 GENERAL

_____. "The People's Information War." p. 84-95, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Khalilzad, Zalmay. "Defense in a Wired World: Protection, Deterrence and Prevention." p. 403-437, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: the Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Kittler, Friedrich. "On the History of the Theory of Information Warfare." p. 266-272, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Knecht, R.J. "Thoughts about Information Warfare" in: Campen, A.D., Dearth, D.H., Thomas Godden, R (eds) **Cyberwar: Security, Strategy, and Conflict in the Information Age**, AFCEA International Press, Fairfax, 1996.
DKL U163 .C94 1996 GENERAL

Komar, David M. **Information-Based Warfare: A Third Wave Perspective**. Maxwell AFB, AL: Air University, Air War College, 1995. 36p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1637

Kopp, Carlo. "Shannon, Hypergames and Information Warfare." Conference Paper, **Proceedings of the 3rd Australian Information Warfare & Security Conference.** Perth, South Australia, 2002.
http://www.csse.monash.edu.au/~carlo/archive/PAPERS/_JIW-2002-1-CK-S.pdf

Kopp, Carlo and Bruce Mills. "Information Warfare and Evolution." Conference Paper. **Proceedings of the 3rd Australian Information Warfare & Security Conference.** Perth, South Australia, 2002.
http://www.csse.monash.edu.au/~carlo/archive/PAPERS/_JIW-2002-2-CK-BIM-S.pdf

Kott, Alexander. **Information Warfare and Organizational Decision-Making**. Boston, MA: Artech House, c2007. 273p.
DKL U163 .I545 2007 GENERAL

Kuehl, Daniel T. **Strategic Information Warfare: A Concept**. Working Paper No, 332. Canberra, Australia: Australian Defence University, Strategic and Defence Studies Centre, 1999. 17p.

Lawrence, R. E. and A. J. Ross. "Equities: Dissemination vs. Protection Information Warfare Workshop Results." p. 566-568, IN: **Proceedings of the First International Symposium on Command and Control Research and Technology.** Washington, DC: National Defense University, 19-22 June 1995. Washington, DC: National Defense University, 1996. 600p.
DKL UB212 .I573 1995 GENERAL

Lesser, Ian O. **Countering the New Terrorism**. Santa Monica, CA: Rand, 1999. 153p.
http://www.rand.org/pubs/monograph_reports/MR989/index.html
DKL UG633 .C68 1999 GENERAL

Levien, Frederic H. **Overview of Information Warfare: Principles and Practice**. Lynx Publishing, November 1999. 32p.

Libicki, Martin C. **Conquest in Cyberspace: National Security and Information Warfare.** New York: Cambridge University Press, 2007. 323p.
DKL U163 .L534 2007 GENERAL

_____. **Defending Cyberspace and Other Metaphors**. Washington, DC: National Defense University, 1997. 110p.
DKL U163 .L52 1997 GENERAL

_____. "Dominate Battlefield Awareness and Its Consequences." p. 550-559, IN: **Proceedings of the First International Symposium on Command and Control Research and Technology.** Washington, DC: National Defense University, 19-22 June 1995. Washington, DC: National Defense University, 1996. 600p.
DKL UB212 .I573 1995 GENERAL

_____. **The Future of Information Security**. Washington, DC: National Defense University, 1998.
http://www.fas.org/irp/threat/cyber/docs/infosec.htm

_____. **The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon**. McNair Paper no. 28. Washington, DC: National Defense University, Institute for National Strategic Studies, 1994. 127p.
http://www.ndu.edu/inss/McNair/mcnair28/mcnair28.pdf
DKL D 5.416:28 FEDDOCS

_____. **What Is Information Warfare?** ACIS Paper No. 3. Washington, DC: National Defense University, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, 1995. 104p.
http://www.ndu.edu/inss/books/Books%20-%201990%20to%201995/What_is_IW_Aug_95/a003.html
DKL U163 .L53 1995 GENERAL

Libicki, Martin and Jeremy Shapiro. "The Changing Role of Information in Warfare." p. 437-452, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Liu, Peng and Sushil Jajodia. **Trusted Recovery and Defensive Information Warfare.** Boston, MA: Kluwer Academic, 2002. 133p.
DKL U 163 .L58 2002 GENERAL

Loundy, David J. **Computer Crime, Information Warfare, and Economic Espionage.** Durham, NC: Carolina Academic Press, 2003. 855p.
DKL KF 9350.A7 L68 2003 GENERAL

Macdonald, Scot. Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations. New York: Routledge, 2007. 204p.
DKL UB275 .M33 2007 GENERAL

Marek, James Raley. **Organizing to Win: Centralized Control for Information Warfare**. Maxwell AFB, AL: Air University, Air Command and Staff College, 2000. 39p.
https://research.maxwell.af.mil/viewabstract.aspx?id=2299

Matthews, Lloyd J. **Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?** Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 1998. 343p.
http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=230

McHale, Michael L. "C2 and NLP: An Information Warfare Perspective." p. 180-185, IN: **Proceedings of the 1996 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 25-28 June 1996. Washington, DC: National Defense University, 1996. 876p.
DKL UB21 .C68 1996 GENERAL

McGuffie, Robert W. "Information Warfare: A New Element of the Conflict Spectrum." p. 126-140, IN: **Proceedings of the 1996 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 25-28 June 1996. Washington, DC: National Defense University, 1996. 876p.
DKL UB21 .C68 1996 GENERAL

McLendon, James W. **Information Warfare: Impact and Concerns**. Maxwell AFB, AL: Air University, Air War College, 1994. 35p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1648

Miller, John H. "Information Warfare: Issues and Perspectives." p. 145-167, IN: Neilson, Robert E. (ed.). **Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition**. Washington, DC: National Defense University Press, 1997. 167p.
http://www.ndu.edu/inss/siws/ch7.html
DKL D 5.402:Su 7 FEDDOCS

Miller, Robert D. **International Law: How it Affects Rules of Engagement and Responses in Information Warfare.** Maxwell AFB, AL: Air University, Air War College, 1997. 40p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1037

Molander, Roger C. **Strategic Information Warfare Rising**. Santa Monica, CA: Rand, 1998. 82p.
http://www.rand.org/pubs/monograph_reports/MR964/index.html
DKL U163 .S756 1998 GENERAL

Molander, Roger C., Peter A. Wilson and Robert H. Anderson. "U.S. Strategic Vulnerabilities: Threats Against Society." p. 253-281, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson. **Strategic Information Warfare: A New Face of War**. Santa Monica, CA: Rand, 1996. 90p.
http://www.rand.org/pubs/monograph_reports/2005/MR661.pdf
DKL U163 .M65 1996 GENERAL

Morris, James R. "Protecting Key Infrastructures and the Impact of the Digital Domain in Information Warfare." p. 642-644, IN: **Proceedings of the Third International Symposium on Command and Control Research and Technology.** National Defense University, Washington, DC, 17-20 June 1997. Washington, DC: National Defense University, 1997. 893p.
DKL UB212 .I573 1997 GENERAL

Munro, Iain. **Information Warfare in Business: Strategies of Control and Resistance in the Network Society.** London; New York: Routledge, 2005. 200p.
DKL HM851 .M86 2005 GENERAL

Munro, Neil. **The Quick and the Dead: Electronic Combat and Modern Warfare**. New York: St. Martins Press, 1991. 324p.
DKL UG485 .M79 1991 GNERAL

National Research Council (U.S.). Naval Studies Board. Committee on Technology for Future Naval Forces. **Technology for the United States Navy and Marine Corps, 2000-2035: Becoming a 21st-Century Force**. Vol. 3. **Information in Warfare**. Washington, DC: National Academy Press, 1997. 131p.
http://www.nap.edu/html/tech_21st/iwindex.htm
DKL VA55 .T42 1997 v. 3 GENERAL

Neilson, Robert E. (ed.). **Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition**. Washington, DC: National Defense University Press, 1997. 167p. *http://www.ndu.edu/inss/siws/cont.html* *OR* *http://www.ndu.edu/inss/siws/STAW.pdf*
DKL D 5.402:Su 7 FEDDOCS

Neilson, Robert E. and Charles B. Giasson "Information -- the Ultimate Weapon." p. 545-549, IN: **Proceedings of the First International Symposium on Command and Control Research and Technology.** Washington, DC: National Defense University, 19-22 June 1995. Washington, DC: National Defense University, 1996. 600p.
DKL UB212 .I573 1995 GENERAL

Nelson, Andrew H. and John Alger I. **The Art of Information War**. [United States]: A.H. Nelson, 1995. 75p.

The New International Security Review 1998. London: Royal United Services Institute for Defence Studies, 1997. 341p.

Nichiporuk, Brian. "U.S. Military Opportunities: Information-Warfare Concepts of Operation." p. 179-215, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p. *http://www.rand.org/pubs/monograph_reports/MR1016/index.html*
DKL UG478 .C43 1999 GENERAL

Nicholson, Peter. **Controlling Australia's Information Environment or Decision Superiority and War-Fighting.** Air Power Studies Centre Paper No. 65. Canberra, Australia: Royal Australian Air Force, Air Power Studies Centre, 1998. 23p.

Noone, James A., et al. **Information Technology for the 21st Century (IT-21) / Historical Documentation Conducted by Naval Reserve Combat Documentation Detachment 206**. [Washington, DC]: Naval Historical Center, 1998.
DKL UB212 .N66 1998 GENERAL

Ochmanek, David A. **To Find and Not to Yield: How Advances in Information and Firepower Can Transform Theater Warfare**. Santa Monica, CA: Rand, 1998. 105p. *http://www.rand.org/pubs/monograph_reports/MR958/*

Panarin, Igor Nicolaevich. "InfoWar and Authority." p. 96-100, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Pfaltzgraff, Robert L. and Richard H. Shultz, Jr. (eds.) **War in the Information Age: New Challenges for U.S. Security Policy**. Washington, DC: Brassey's, 1997. 375p.
DKL U104 .W37 1997 GENERAL

Planning Considerations for Defensive Information Warfare: Information Assurance / prepared for Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Organization (JIEO), Center for Information Systems Security (CISS). [S.l. : s.n., 1993] 61p.
http://handle.dtic.mil/100.2/ADA392657

Pufeng, Wang. "The Challenge of Information Warfare." p. 317-326, IN: Pillsbury, Michael (ed.). **Chinese Views of Future Warfare**. Washington, DC: National Defense University Press, 1997. 421p.
http://www.ndu.edu/inss/books/Books%20-%201998/Chinese%20Views%20of%20Future%20Warfare%20-%20Sept%2098/chinapt4.html#7
DKL UA835 .C453 1997 GENERAL

Rathmell, Andrew, et al. "The IW Threat from Sub-State Groups: An Interdisciplinary Approach." p. 164-177, IN: **Proceedings of the Third International Symposium on Command and Control Research and Technology.** National Defense University, Washington, DC, 17-20 June 1997. Washington, DC: National Defense University, 1997. 893p.
DKL UB212 .I573 1997 GENERAL

Rattray, Gregory J. "The Global Information Infrastructure, National Security and Cooperative Approaches." p. 707-736, IN: **Proceedings of the Third International Symposium on Command and Control Research and Technology.** National Defense University, Washington, DC, 17-20 June 1997. Washington, DC: National Defense University, 1997. 893p.
DKL UB212 .I573 1997 GENERAL

_____. **Strategic Information Warfare: Challenges for the United States**. (Ph.D thesis – Fletcher School of Law and Diplomacy). Wright-Patterson AFB, OH: Air Force Institute of Technology, 1998. 704p.

Rowe, Wayne. **Information Warfare: A Primer for Navy Personnel.** Newport, RI: Naval War College, Center for Naval Warfare Studies, June 1995. 34p.

Rushkoff, Douglas. "Coercion and Countermeasures: The Information Arms Race." p. 218-227, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Salomone, Michael D., John P. Crecine and Alethia H. Cook. "Strategic Perspectives on Information Technologies and Information Warfare." p. 156-168, IN: **Proceedings of the 1996 Command and Control Research and Technology Symposium.** Monterey, CA: Naval Postgraduate School, 25-28 June 1996. Washington, DC: National Defense University, 1996. 876p.
DKL UB212 .C68 1996 GENERAL

Schleher, D. Curtis. **Electronic Warfare in the Information Age**. Boston, MA: Artech House, 1999. 605p.
DKL UG485 .S3497 1999 GENERAL

Schofbanker, Georg. "From Plato to NATO." p. 101-118, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Schwartau, Winn. **Information Warfare: Chaos on the Electronic Superhighway**. New York: Thunder's Mouth Press; Emeryville, CA: Distributed by Publishers Group West, c1994. 432p.
DKL QA76.9 .A25 S354 1994 GENERAL

_____. **Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age**. 2nd ed. New York: Thunder's Mouth Press; Emeryville, CA: Distributed by Publishers Group West, c1996. 768p.
DKL QA76.9 .A25 S354 1996 GENERAL

Schwartzstein, Stuart J. D., ed. **The Information Revolution and National Security Dimensions and Directions**. (Significant Issues Series, v.18, no.3). Washington, DC: Center for Strategic & International Studies, 1996. 263p.
DKL UA23 .I39 1996 GENERAL

Shapiro, Jeremy. “Information and War: Is It a Revolution?” p. 113-153, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Siegel, Pascale-Combelles. **Target Bosnia: Integrating Information Activities in Peace Operations: NATO-Led Operations in Bosnia-Herzegoviona, December 1995-1997**. Washington, DC: National Defense University, 1998. 199p.
http://www.dodccrp.org/files/Siegel_Target.pdf
DKL DR1313.7 .P73 1998 GENERAL

Smith, Anthony C. **Operation Integration of Information Warfare.** Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 17p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1011

Soo Hoo, Kevin J. **Strategic Information Warfare: A New Arena for Arms Control?** Stanford, CA: Stanford University, Institute for International Studies, Center for International Security and Arms Control, 1997. 12p.

Sovereign, Michael G. “Warfare in the Information Age: Vision 2010 and Changes in Joint C4 Doctrine.” p. 141-147, IN: **Proceedings of the 1996 Command and Control Research and Technology Symposium.** Monterey, CA: Naval Postgraduate School, 25-28 June 1996. Washington, DC: National Defense University, 1996. 876p.
DKL UB212 .C68 1996 GENERAL

Stanley, Elizabeth A. **Evolutionary Technology in the Current Revolution in Military Affairs: The Army Tactical Command and Control System**. Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1998. 67p.
http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=232

Starr, Stuart H. and Dale K. Pace. “Developing the Intellectual Tools Needed By the Information Warfare Community.” p. 577-588, IN: **Proceedings of the First International Symposium on Command and Control Research and Technology.** Washington, DC: National Defense University, 19-22 June 1995. Washington, DC: National Defense University, 1996. 600p.
DKL UB212 .I573 1996 GENERAL

Stein, George J. **Information Attack: Information Warfare In 2025**. Air Force 2025 series. Maxwell AFB, AL: Air University, Air War College, 1996. 41p.
http://csat.au.af.mil/2025/volume3/vol3ch03.pdf

_____. "Information Warfare: Words Matter." p. 51-59, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Stein, George and Szafranski, Richard. **US Information Warfare**. Alexandria, VA: Jane's Information Group, 1996. 218p. (Jane's special report)
DKL U163 .S73 1996 GENERAL

Stevens, William K., William L. Decker and Colleen M. Gagnon. “Representation of C2 and IW in Military Simulations.” p. 240-255, IN: **Proceedings of the Second International Symposium on Command and Control Research and Technology.** Market Bosworth, United Kingdom, 24-26 June 1996. Washington, DC: National Defense University, 1997. 592p.
DKL UB212 .I573 1996 GENERAL

_____. “Representation of Command and Control and Information Warfare in Military Simulations.” p. 40-55, IN: **Proceedings of the 1996 Command and Control Research and Technology Symposium.** Monterey, CA: Naval Postgraduate School, 25-28 June 1996. Washington, DC: National Defense University, 1996. 876p.
DKL UB212 .C68 1996 GENERAL

Stewart John and John Corder. "Information in Warfare: Toward Dynamic Command and Control." p. 72-79, IN: **Information Applications Volume, New World Vistas: Air and Space Power in the 21st Century**, [Washington, DC?: USAF Scientific Advisory Board, 1995-]
DKL D 301.118:P 87/2/INFORM FEDDOCS

Stocker, Gerfried. "Info War." p. 11-23, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Stokes, Mark A. **China's Strategic Modernization: Implications for the United States**. Carlisle Barracks, PA: Army War College, Strategic Studies Institute, 1999. 229p. *http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?PubID=74*

Sullivan, Gordon R. and James M. Dubik. **War in the Information Age**. Carlisle Barracks, PA: Army War College, Strategic Studies Institute, 1994. 23p.
http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?PubID=243

Thom, Maxie C. **Information Warfare Arms Control: Risks and Costs.** INSS Occasional Paper, no. 63. USAF Academy, CO: USAF Institute for National Security Studies, [2006]. 66p.
DKL D 305.24:63 FEDDOCS
http://www.usafa.af.mil/df/inss/OCP/ocp63.pdf

Thomas, Timothy L. **Behind the Great Firewall of China: A Look at RMA/IW Theory From 1996-1998**. Ft. Leavenworth, KS: Foreign Military Studies Office, 1998.
http://fmso.leavenworth.army.mil/documents/chinarma.htm

_____. **Dragon Bytes: Chinese Information-War Theory and Practice From 1995-2003**. Fort Leavenworth, KS: Foreign Military Studies Office, 2004. 168p.

_____. "Information Technology: US/Russian Perspectives and Potential for Military-Political Cooperation." p. 69-89. IN: Cross, Sharyl et al (eds.) **Global Security Beyond the Millennium**. New York: St Martins Press, 1999, 260p.

Toffler, Alvin. **The Third Wave**. New York: Bantam Books, 1981. 537p.
DKL HN17.5 .T643 GENERAL

Toffler, Alvin and Heidi. **War and Anti-War: Survival at the Dawn of the 21st Century**. Boston: Little, Brown, 1993. 302p.
DKL U102 .T64 1993 GENERAL

United States. Air Force. **Cornerstones of Information Warfare**. [Washington, D.C.?] : Dept. of the Air Force, [1995?] 13p.
http://handle.dtic.mil/100.2/ADA323807

United States. Air Force. [HQ USAF/XOXD (Air Force Doctrine Division)] **Information Warfare.** [Washington, D.C.?] : Dept. of the Air Force, [1996?] 16p.

United States. Air Force Information Warfare Center. **Air Force Information Warfare Center**. Kelly Air Force Base, TX: Air Force Information Warfare Center, [1996?] 37p.

United States. Congress. Senate. Select Committee on Intelligence. **Current and Projected National Security Threats to the United States: Hearing Before the Select Committee on Intelligence of the United States Senate, One Hundred Fifth Congress, Second Session ... Wednesday, January 28, 1998.**. Washington, DC: GPO, 1998. 177p.
DKL Y 4.IN 8/19:S.hrg. 105-587 FEDDOCS

United States. Defense Science Board. **Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D).** Washington, DC: Office of the Under Secretary of Defense for Acquisition & Technology, 1996.
http://cryptome.org/iwd.htm
http://handle.dtic.mil/100.2/ADA319571

United States. Defense Science Board. **Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield**. Washington, DC: Office of the Under Secretary of Defense for Acquisition & Technology, 1994.
http://handle.dtic.mil/100.2/ADA286745
DKL U164 .U54 1994 GENERAL

United States. Joint Chiefs of Staff. **Defensive Information Warfare Implementation**. CJCSI 6510.01A [Washington, D.C.] : Joint Chiefs of Staff, [1996]

United States. Joint Chiefs of Staff. **Information Warfare: A Strategy for Peace: The Decisive Edge in War**. [Washington, D.C.?] : Joint Chiefs of Staff, [1996 and 1999] 19p.
http://handle.dtic.mil/100.2/ADA318379
DKL D 5.2:In 3 FEDDOCS

United States. Office of the Chief of Naval Operations. **Information Warfare Strategic Plan: Navy IW: IW, Capabilities for the New Millennium**. [Washington, DC: U.S. Navy, Chief of Naval Operations, 1998?] 19p.
DKL D 201.2:IN 3/2 FEDDOCS

United States. President's Commission on Critical Infrastructure Protection. **Critical Foundations: Protecting America's Infrastructures**. Washington, DC, 1997. 102p.
http://chnm.gmu.edu/cipdigitalarchive/files/5_CriticalFoundationsPCCIP.pdf
DKL PR 42.8:IN 3/C 86 FEDDOCS

Vadnais, Daniel M. **Law of Armed Conflict and Information Warfare – How Does the Rule Regarding Reprisals Apply to an Information Warfare Attack?** Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 27p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1010

Waltz, Edward. **Information Warfare: Principles and Operations**. Boston, MA: Artech House, c1998. 397p.
DKL U163 .W38 1998 GENERAL

Weiguang, Shen. "Information Warfare: A New Challenge." p. 60-83, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Wells, Daniel W. **Information Warfare in a Joint and National Context**. Maxwell AFB AL: Air University, Air War College, April 1996. 27p.

Westwood, Chris. **The Future is Not What It Used to Be: Conflict in the Information Age**. Fellowship paper no. 13. Canberra: Australia: Royal Australian Air Force. Air Power Studies Centre, 1997. 152p.

Wheatley Gary F. and Richard E. Hayes. **Information Warfare and Deterrence**. Washington, National Defense University. Institute for National Strategic Studies, 1996. 93p.
http://www.dodccrp.org/files/Wheatley_Deterrence.pdf

Whitehead, YuLin G. **Information as a Weapon: Reality Versus Promises.** Maxwell Air Force Base, AL: Air University Press, School of Advanced Airpower Studies, 1997. 39p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1297

Wilson, Clay. **Information Warfare and Cyberwar: Capabilities and Related Policy Issues.** RL31787. Washington, DC: Congressional Research Service, Library of Congress, 2006.
http://bosun.nps.edu/uhtbin/hyperion-image.exe/CRS-RL31787.pdf

Wilson, Michael. "National Security and Infrastructural Warfare." p. 119-193, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Winkler, J. R., C. J. O'Shea and M. C. Stokrp. "Information Warfare and Dynamic Information Defense." p. 169-179, IN: **Proceedings of the 1996 Command and Control Research and Technology Symposium.** Monterey, CA: Naval Postgraduate School, 25-28 June 1996. Washington, DC: National Defense University, 1996. 876p. **DKL UB212 .C68 1996 GENERAL**

Wood, Robert J. **Information Engineering: The Foundation of Information Warfare**. Maxwell AFB, AL: Air University, 1995. 67p. *https://research.maxwell.af.mil/viewabstract.aspx?id=1671*

Periodicals

“609th Information Warfare Squadron: Shaw Air Force Base, S.C.” **Air Force Times**, August 11, 1997, v. 58, no. 1, p. 33.

Ackerman, Robert K. “Bytes Transform Army, Turn Service Roles Upside Down.” **Signal**, May 1994, v. 48, no. 9, p. 21-24.

_____. “Bandwidth Demands Portend Revolutionary Program Taxes.” **Signal**, June 1998, v. 52, no. 10, p. 25-26+

_____. "Businesses Face Threat of Information Warfare." **Signal**, June 1996, v. 50, no. 10, p. 45-46.

_____. "Command, Control Simulation Develops Information Warriors." **Signal**, February 1997, v. 51, no. 6, p. 25-28.

_____. "Digital Formats Complicate Information Security Tasks." **Signal**, February 1997, v. 51, no. 6, p. 21-23.

_____. “Europe Seeks Overarching View of Information War.” **Signal**, July 1998, v. 52, no. 11, p. 33-35.

_____. ”Hidden Hazards Menace U.S. Information Infrastructure.” **Signal**, August 1999, v. 53, no. 12, p. 17-20.

_____. “Information Age Poses New Challenges to Intelligence.” **Signal**, October 1998, v. 53, no. 2, p. 23-25.

_____. “Information Officers Disseminate, Protect Intelligence Agency Data.” **Signal**, July 1997, v. 51, no. 11, p. 59-62.

_____. “Justice Department Readies Infrastructure Defense Plans.” **Signal**, July 1998, v. 52, no. 11, p. 17-19.

_____. “Kosovo Maps the Future of Information Technologies.” **Signal**, December 1999, v. 54, no. 4, p. 49-54.

_____. "Microscopic Magicians Wage Information Security Skirmish." **Signal**, July 1997, v. 51, no. 11, p. 35-37.

_____. "Military Planners Gird for Information Revolution." **Signal**, May 1995, v. 49, no. 9, p. 71-76.

_____. "Marine Crops Information Warfare Combines Services’ Needs, Defines Their Differences." **Signal**, July 1996, v. 50, no. 11, p. 61-62.

_____. "Navy Doctrine, Systems Face Information Warfare Makeover." **Signal**, July 1996, v. 50, no. 11, p. 57-60.

Adam, John A. “Warfare in the Information Age.” **IEEE Spectrum**, September 1991, v. 28, no. 9, p. 26-33.

Adams, Charlotte. “DOD Information Security Takes Big Strides But Still Lags Behind Threats.” **Military & Aerospace Electronics**, January 1997, v. 8, no. 1, p. 17-19.

_____. “Information Warfare Takes a Front Seat.” **Military & Aerospace Electronics**, June 1996, v. 7, no. 6, p. 19-21.

Adams, Thomas K. “Radical Destabilizing Effects of New Technologies.” **Parameters**, Autumn 1998, v. 28, no. 3, p. 99-111.

Aftergood, Steven. “The Soft-Kill Fallacy.” **Bulletin of the Atomic Scientists**, September/October 1994, v. 50, no. 5, p. 40-45.

Ahari, M. Ehsan. "China Changes Its Strategic Mindset.” **Jane’s Intelligence Review**, Pt. 1, November 1999, v. 11, no. 11, p. 38-44, Pt. 2., December 1999, v. 11, no. 12, p. 30-35.

_____. "Chinese Prove to be Attentive Students of Information Warfare." **Jane's Intelligence Review**, October 1997, v. 9, no. 10, p. 469-473.

_____. “U.S. Military Strategic Perspectives on the PRC: New Frontiers of Information-Based War.” **Asian Survey**, December 1997, v. 37, no. 12, p. 1163-1180.

Aldrich, Richard W. "The International Legal Implications of Information Warfare." **Airpower Journal**, Fall 1996, v. 10, no. 3, p. 99-110.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/fall96/aldricha.html OR
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/fall96/aldrich.pdf

Alexander, David. "From Cyberspace to Battlespace: Information Warfare and the Electronic Order of Battle." **Military Technology**, December 2003, v. 27, no. 12, p. 44-46+

Alexander, David. "Information Warfare and the Digitized Battlefield." **Military Technology**, September 1995, v. 19, no. 9, p. 57-59+

Alexander, John B. “Nonlethal Weapons: When Deadly Force is Not Enough.” **The Futurist**, October 1999, v. 33, no. 8, p. 34-38.

Alger, John I. "Declaring Information War: Early Training Crucial to Awareness." **International Defense Review**, July 1996, v. 29, no. 7, p. 54-55.

_____. "From Hackers to Projectors of Power." **Bulletin of the American Society for Information Science**, October/November 1996, v. 23, no. 1, p. 6-8.

Allard, Kenneth. “Assessing ‘Byte City’: An Insightful or Misleading Vision?” **Washington Quarterly**, Spring 1997, v. 20, no. 2, p. 84-93. [this is a response to the Vlahos article]

Anderson, Emory A. and Cynthia E. Irvine and Roger R. Schell. “Subversion as a Threat in Information Warfare.” **Journal of Information Warfare**, June 2004, v. 3, no. 2, p. 52-65.
http://www.nps.navy.mil/cs/facultypages/faculty/irvine/Publications/Publications2004/Subversion_JIW_2.pdf

Anderson, Gary W. and Terry C. Pierce. "Leaving the Technocratic Tunnel." **Joint Force Quarterly**, Winter 1995-1996, no. 10, p. 69-75.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1710.pdf

Andrews, C. “Belief Systems, Information Warfare, and Counter Terrorism.” **Journal of Information Warfare**, March 2005, v. 4, no. 1, p. 41-48.

Anthes, Gary H. "DOD on Red Alert to Fend Off Info Attacks." **Computerworld**, January 6, 1997, v. 31, no. 1, p. 1+

_____. “Feds Limit Info Warfare Role.” **Computers & Security**, 1995, v. 14, no. 16, p. 522.

_____. "Info Warfare Risk Growing." **Computerworld**, May 22, 1995, v. 29, no. 21, p. 1+

_____. "New Laws Sought for Info Warfare." **Computerworld**, June 5, 1995, v. 29, no. 23, p. 55+

_____. "Security Pundits Weigh War Threat." **Computerworld**, October 2, 1995, v. 29, no. 40, p. 71+

_____. “U.S. Easy Target for Cyberattacks.” **Computerworld**, May 27, 1996, v. 30, no. 22, p. 7.

Anthony, Keith D. “Information Warfare: Good News and Bad News.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 31-34.

Arnett, Eric H. “Welcome to Hyperwar.” **Bulletin of the Atomic Scientists**, September 1992, v. 48, no. 7, p. 14-21.

Arnold, Wallace C. and Thomas H. Killion. "MANPRINT (Manpower and Personnel Integration): Battle Command and Digitization." **Military Review**, May-June 1995, v. 75, no. 3, p. 48-55.

_____. "The Soldier-Information Interface." **Army RD&A Bulletin**, January 1995, no. 1, p. 7-9.

Arquilla, John. "Can Information Warfare Ever be Just?" **Ethics and Information Technology**, 1999, v. 1, no. 3, p. 203-212.

_____. "Strategic Information Warfare." **Comparative Strategy**, October 1996, v. 15, no. 4, p. 387-388.

"Attack Software Plays Key Offensive Role." **Aviation Week & Space Technology**, January 19, 1998, v. 148, no. 3, p 56.

Ayers, Robert. "The New Threat: Information Warfare." **RUSI Journal**, October 1999, v. 144, no. 5, p. 23-27.

Bacevich, Andrew J. "Assessing 'Byte City': An Insightful or Misleading Vision?" **Washington Quarterly**, Spring 1997, v. 20, no. 2, p. 78-80. [this is a response to the Vlahos article]

Bacon, Michael. "The Enemy Everywhere." **Computers & Security**, 1997, v. 16, no. 6, p. 516.

Baines, Thomas B., Chris Morris and Janet Morris. "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos." **Airpower Journal**, Spring 1995, v. 9, no.1, p. 15-29. *http://www.airpower.maxwell.af.mil/airchronicles/apj/morris.html*

Banford, Harry C. and Paul L. High. "Intelligence Communications in the Age of Information Warfare." **American Intelligence Journal**, Autumn/Winter 1994, v. 15, no. 2, p. 52-57.

Bangkok, Robert Karniol. "Myanmar Spy Centre Can Listen in to Sat-Phones." **Jane's Defence Weekly**, September 17, 1997, v. 28, no. 11, p. 18.

Barlow, John P. "A Taxonomy of Information." **Bulletin of American Society for Information Science**, June-July 1994, v. 20, no. 5, p. 13-17.

Barwinczak, Patricia M. "The Information Revolution and Warfare 2020." **Strategic Review**, Spring 1997, v. 25, no. 2, p. 77-79.

Bateman, Robert L. "Avoiding Information Overload." **Military Review**, July-August 1998, v. 78, no. 4, p. 53-58.

_____. “Force XXI and the Death of Auftragstaktik.” [Examines the issue of Information Warfare] **Armor**, January-February, 1996, v. 105, no. 1, p. 13-15.

Bates, James C. “UltraLog: Securing Logistics Information on the Battlefield.” **Army Logistician**, March-April 2005, v. 37, no. 2, p. 19-23. *http://www.almc.army.mil/alog/issues/MarApr05/Ultralog.html*

Bates, Troy R. "Internet Support to Expeditionary Forces: Filling the Intelligence Gap." **Marine Corps Gazette**, June 1997, v. 81, no. 6, p. 41-43.

Bean, Mark H. “Fourth Generation Warfare?” **Marine Corps Gazette**, March 1995, v. 79, no. 3, p. 53-54.

Belen, Fred C. "Littoral Battlespace ACTD (Advanced Concept Technology Demonstration) Offers Clear Combat Edge." **National Defense,** April 1998, v. 82, no. 537, p. 48-49.

Bender, Brian. “Defense Review Vows ‘Robust Commitment’ to Information Warfare.” **Defense Daily**, June 3, 1997, v. 195, no. 45, p. 1.

_____. “Rising Cyber Attacks Force Development of ‘Tolerant’ Networks.” **Jane’s Defence Weekly**, November 3, 1999, v. 32, no. 18, p. 27.

Bergman, Kenneth R. "Space and the Revolution in Military Affairs." **Marine Corps Gazette**, May 1995, v. 79, no. 5, p. 58-60.

Berkowitz, Bruce. “Information Warfare: Time to Prepare.” **Issues in Science**, Winter 2000/2001, v. 17, no. 2, p. 37-44.

Berkowitz, Bruce D. "Warfare in the Information Age." **Issues in Science and Technology**, Fall 1995, v. 12, no. 1, p. 59-66.

Betz, David J. “The More You Know, the Less You Understand: The Problem with Information Warfare.” **Journal of Strategic Studies**, June 2006, v. 29, no. 3, p. 505-533.

Bigelow, Brad. “Forces, Targets, and Effects: Militarising Information Warfare.” **Journal of Information Warfare**, October 2002, v. 2, no. 1.

Black, Peter. “Soft Kill: Fighting Infrastructure Wars in the 21st Century.” **Wired**, July-August 1993, v. 1, no. 3, p. 49-50. *http://www.wired.com/wired/archive/1.03/1.3_softkill.html*

Blaker, Jim. "The Owens Legacy: The Former Vice Chairman of the Joint Chiefs Laid the Groundwork for a Revolution." **Armed Forces Journal International**, July 1996, v. 133, no. 12, p. 20-22.

Blank, Stephen. “Can Information Warfare be Deterred?” **Defense Analysis**, August 2001, v. 17, no. 2, p. 121-138.

Blazer, Ernest. “Planners: Information is the Best Weapon.” **Navy Times**, September 5, 1994, v. 43, no. 48, p. 8.

Blenkin, M. “Information Warfare Could be Way of Future Conflict.” **Search**, July 1996, v. 27, no. 6, p. 172+

Blount, Kerry A. "Two-Part Component Strategy for Winning the Information War." **Army**, January 1995, v. 45, no. 1, p. 10+

_____. "Wrestling with Information Warfare's 'Dark Side.'" **Army**, February 1996, v. 46. no. 2, p. 9+

Blount, Kerry A. and Lauren D. Kohn. “C2 Warfare in FM 100-6.” **Military Review**, July/August 1995, v. 75, no. 4, p. 66-69.

Boatman, John. “ARPA Sharpens Up for Information Warfare.” **Jane’s Defence Weekly**, August 19, 1995, v. 24, no. 7, p. 5.

Bodnar, John W. “Military-Technical Revolution: From Hardware to Information.” **Naval War College Review**, Summer 1993, v. 46, no.3, p. 7-21.

Boldrick, Michael R. “Information Warfare: The Next Major Change in Military Strategies and Operational Planning.” **Soldier-Scholar**, Fall 1996, v. 3, no. 3, p. 11-19.

Boorda, Jeremy M. "Leading the Revolution in C4I (Command, Control, Communications, Computer, and Intelligence)." **Joint Force Quarterly**, Autumn 1995, no. 9, p. 14-17.
http://www.dtic.mil/doctrine/jel/jfq_pubs/0809.pdf

“Bosnia's Information River Slows, Trickles to Soldiers.” **Signal**, June 1997, v. 51, no. 10, p. 87-90.

Bolt, Paul J. and Carl N. Brenner. “Information Warfare Across the Taiwan Strait.” **Journal of Contemporary China**, February 2004, v. 13, no. 38, p. 129-150.

Boulanger, A. "Catapults and Grappling Hooks: The Tools and Techniques of Information Warfare." **IBM Systems Journal**, 1998, v. 37, no. 1, p. 106-114.

Bowdish, Randall G. "The Revolution in Military Affairs: The Sixth Generation." **Military Review**, November/December 1995, v. 75, no. 6, p. 26-33.

Bowers, Stephen R. “Information Warfare: The Computer Revolution is Altering How Future Wars Will be Conducted.” **Armed Forces Journal International**, August 1998, v. 136, no. 1, p. 38-39.

Braunberg, Andrew C. "Air Force Pursues Two-Sided Information Warfare Strategy." **Signal**, July 1996, v. 50, no. 11, p. 63-65.

Bristow, Damon. “TECHNOLOGY - Information Warfare Grips China.” [Pointer Edition], **Jane's Intelligence Review**, November 1, 1998, v. 5, no. 11, p. 8.

Brohm, Gerard P. “C4IEWS in the US Army – Issues, Analysis, and Trends.” **NATO’s Sixteen Nations**, 1997, v. 42, no. 3, p. 64-66.

Broucek, Vlasti and Paul Turner. “Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare.” **Journal of Information Warfare**, December 2001, v. 1, no. 2, p. 95-108.

Brown, Charlie G. “Catch the Train.” **Journal of Electronic Defense**, June 1997, v. 20, no. 6, p. 12+

Brown, Christopher E. “The "Q" Transition.” **United States Naval Institute Proceedings**, February 1997, v. 123, no. 2, p. 57-61.

Brown, David and John Burlage. “Navy Molding Enlisted Into Tech-Savvy Sailors.” **Navy Times**, July 26, 1999, v. 48, no. 42, p. 16.

Brown, George C.L. “Do We Need FA30? Creating an Information Warfare Branch.” **Military Review,** January-February 2005, v. 85, no. 1, p. 39-43. *http://usacac.army.mil/cac/milreview/download/english/JanFeb05/Bbro.pdf*

Browning, Graeme. “Counting Down.” **National Journal**, April 19, 1997, v. 29, no. 16, p. 746-749.

Bulloch, Gavin. "The Application of Military Doctrine to Counterinsurgency (COIN) Operations: A British Perspective." **Studies in Conflict and Terrorism**, July-September 1996, v. 19, no. 3, p. 247-259.

Bunker, Robert J. “Generations, Waves, and Epochs and the RPMA.” **Airpower Journal**, Spring 1996, v. 10, no. 1, p. 18-28. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/spr96/bunker.pdf*

_____. “Higher-Dimensional Warfighting.” **Military Review**, September/October 1999, v. 79, no. 5, p. 53-62.

_____. "Transition to Fourth Epoch War." **Marine Corps Gazette**, September 1994, v. 78, no. 9, p. 20.

Bunkers, Frank. "Uncorking the Information Genie." **Marine Corps Gazette**, October 1995, v. 79, no. 10, p. 29-31.

Burgess, Sean P. “Industry, Government Pursue Data Security Clearinghouse.” **Signal**, March 1997, v. 51 no. 7, p. 69-71.

Burke, Charles M. "'Bondage' of Tradition (to Principles, Procedures and Protocols)." **Military Review**, July-August 1995, v. 75, no. 4, p. 10-12.

Burnette, Gerald. “Information: the Battlefield of the Future.” **Surface Warfare**, July-August 1995, v. 20, no. 4, p. 8-9.

Busey, James B., IV. “Battlefield Technologies Muster in Synthetic Arenas.” **Signal**, July 1995, v. 49, no. 11, p. 15.

_____. "Information Warfare Calculus Mandates Protective Actions." **Signal**, February 1994, v. 49, no. 2, p. 15+

_____. “Integral Security Mechanisms are Priority, not Afterthought.” **Signal**, October 1995, v. 50, no. 2, p. 13.

”Businesses Face Threat of Information Warfare." **Signal**, June 1996, v. 50, no. 10, p. 45-46.

Busuttil, Tyrone B. and Matt J. Warren. “Intelligent Agent Technology Within Information Warfare.” **Journal of Information Warfare**, December 2001, v. 1, no. 2, p. 52-61.

Callum, Robert. “Will Our Forces Match the Threat?” **United States Naval Institute Proceedings**, August 1998, v. 124, no. 8, p. 50-53.

Camacho, Paul R. "Managing ‘Command and Control’ in the Persian Gulf War." **Armed Forces and Society**, Winter 1997, v. 24, no. 2, p. 335-338.

Campen, Alan D. “Assessments Necessary in Coming to Terms with Information War.” (Commentary). **Signal**, June 1996, v. 50, no. 10, p. 47-49.

_____. "Cooperative Effort Encourages Safe Information Highway Travel." **Signal**, October 1995, v. 50, no. 2, p. 43-44.

_____. “Information Age Warfare Must Enlist Civilian Partnerships.” **Signal**, June 1999, v. 53, no. 10, p. 65-66+

_____. "Information Warfare is Rife With Promise, Peril." **Signal**, November 1993, v. 48, no. 3, p. 19-20.

_____. "Information Warfare Techniques Supercede Kinetic Weapons." **Signal**, May 1998, v. 52, no. 9, p. 33-36.

_____. “It’s Vulnerability, Not Threat-Stupid!” **Signal**, September 1997, v. 50, no. 1, p. 69-70.

_____. "Joint Vision Initiates Big Challenge to Acquisition, Integration, Culture." **Signal**, October 1997, v. 52, no. 2, p. 71-73.

_____. “National Vulnerability Intensifies as Infrastructure Reliance Grows.” **Signal**, July 1998, v. 52, no. 11, p. 20-22.

_____. "Rush to Information-Based Warfare Gambles with National Security." **Signal**, July 1995, v. 49, no. 11, p. 67-69.

_____. "Vulnerability of Info Systems Demands Immediate Action." **National Defense**, November 1995, v. 80, no. 512, p. 26-27.

Capaccio, Tony and Mary Greczyn. "Warfare in the Information Age." **Popular Science**, July 1996, v. 249, no. 1, p. 52-57.

Caravella, Frank J. “Achieving Sensor-to-Shooter Synergy.” **Military Review**, July-August 1998, v. 78, no. 4, p. 59-64.

_____. "ADA's (Air Defense Artillery's) Role in Winning the Information War." **ADA [Air Defense Artillery]**, September-October 1995, p. 2-3.

Carlin, John. “The Netizen: A Farewell to Arms.” **Wired**, May 1997, v. 5, no. 5, p. 51. *http://www.wired.com/wired/archive/5.05/netizen.html*

Carroll, Bonnie C. "Information Warfare: Military Doctrine and Economic Reality.” **Bulletin of the American Society for Information Science**, October/November 1996, v. 23, no. 1, p. 5.

Caruth, Greg and J. Collie Johnson. "Program Manager Interviews Anita Jones, Director, Defense Research and Engineering." **Program Manager**, July-August 1996, v. 25, no. 4, p. 2-8.

Carver, Curtis A., Jr. “Information Warfare: Task Force XXI or Task Force Smith?” **Military Review**, September-November 1998, v. 78, no. 5, p. 26-30.

Casper, Lawrence E., et al. "Knowledge-Based Warfare: A Security Strategy for the Next Century." **Joint Force Quarterly**, Autumn 1996, no. 13, p. 81-89. *http://www.dtic.mil/doctrine/jel/jfq_pubs/1813.pdf*

Cassidy, Timothy J. "Information Security Awareness: Every Marine's Responsibility." **Marine Corps Gazette**. April 1998, v. 82, no. 4, p. 57-58.

Cebrowski, Arthur K. “C4I in the US Navy: A Look into the 21st Century.” **NATO’s Sixteen Nations**, 1997, v. 42, no. 3, p. 56-59.

Celko, Joe. “Battle of Bits.” **Intelligent Enterprise**, May 11, 1999, v. 2, no. 7, p. 72+

Cerjan, Paul G. and Robert B. Clarke. “NDU Develops a Discipline in Information-Based Warfare.” **Army**, May 1994, v. 44, no. 5, p. 18-19.

Chaisson, Kernan. “Intel Community Gets Involved in Countering IW Threat.” **Journal of Electronic Defense**, February 1999, v. 22, no. 2, p. 18.

Chambers, Elai C. “Information Warfare: Protecting the Chief's Network!” **TIG Brief**, November-December 1996, v. 48, no. 6, p. 10-13.

Chandler, Clifford E., III and Diane Palermo. “NSWC and the Information Revolution.” **Surface Warfare**, July/August 1995, v. 20, no. 4, p. 36-40.

Chenery, John T. “Transnational Threats 101: Today’s Asymmetric Battlefield.” **Military Intelligence Profession Bulletin**, July-September 1999, v. 25, no. 3, p. 4-9.

“CIA Warns Against ‘Information Warfare.’” **Educational Review**, September/October 1998, v. 33, no. 5, p. 10+

Cilluffo, F. and C. Gergely. “Information Warfare and Strategic Terrorism.” **Terrorism and Political Violence**, Spring 1997, v. 9, no. 1, p. 84-94.

Cimbala, Stephen J. “Accidental/Inadvertent Nuclear War and Information Warfare.” **Armed Forces and Society**, Summer 1999, v. 25, no. 4, p. 653-675.

_____. “Information Warfare and Nuclear Conflict Termination.” **European Security**, Winter 1998, v. 7, no. 4, p. 69-90.

_____. “Information Warfare and Nuclear Preemption.” **National Security Studies Quarterly**, Spring 1998, v. 4, no. 2, p. 1-13.

_____. “Nuclear Crisis Management and Information Warfare.” **Parameters**, Summer 1999, v. 29, no. 2, p. 117-128. *http://carlisle-www.army.mil/usawc/Parameters/99summer/cimbala.htm*

Clapper, James R., Jr. and Eben H. Trevino, Jr. "Critical Security Dominates Information Warfare Moves." **Signal**, March 1995, v. 49, no. 7, p. 71-72.

Clauer, John A. "Unified Effort in Support of Dominant Maneuver on the Joint Battlefield." **Marine Corps Gazette**, October 1997, v. 81, no. 10, p. 52-58.

Cline, Mary Ann. “Information Warfare.” **Defense Intelligence Journal**, Spring 1996, v. 5, no.1, p. 83-86.

Clodfelter, Mark and John M. Fawcett, Jr. "RMA (Revolution in Military Affairs) and Air Force Roles, Missions, and Doctrine." **Parameters**, Summer 1995, v. 25, no. 2, p. 22-29.

Cohen, Eliot A. “A Revolution in Warfare.” **Foreign Affairs**, March/April 1996, v. 75, no. 2, p. 37-54.

Cohen, Fred. “Managing Network Security: In Your Face Information Warfare.” **Computer Fraud & Security**, 1999, v. 1999, no. 9, p. 8-10.

Colucci, Frank. “Using Data as a Weapon.” **Rotor & Wing**, August 1994, v. 28, no. 8, p. 23-27.

“Command, Control Simulation Develops Information Warriors.” **Signal**, February 1997, v. 51, no. 6, p. 25-28.

"Commanders Pull Intelligence Information Warfare Strategy." **Signal**, August 1994, v. 48, no. 12, p. 29-31.

“Commercial, Military Information Security Requirements Meld.” **Signal**, May 1996, v. 50, no. 9, p. 108-109.

“Commercial Systems Enhance Information Warfare Capability.” **Signal**, March 1997, v. 51, no. 7, p. 64-65.

Constance, Paul. “From Bombs to Bytes: Era of On-Line Weaponry is Here.” **Government Computer News**, October 2, 1995, v. 14, no. 21, p. 51.

_____. “Center Sics a Digital Bloodhound on Network Intruders.” **Government Computer News**, July 17, 1995, v. 14, no. 14, p. 20.

Cook, Nick. "BattleSpace 2000: Fighting for a Share of the Infowar Market.” **Interavia**, June-July 1996, v. 51, no. 601, p. 43-45.

_____. “Big Question: Can Saddam be Beaten by Bombing Alone?” **Jane’s Defence Weekly**, February 25, 1998, v. 29, no. 8, p. 20-21.

_____. "USAF Plans the Next Age of Warfighting." **Jane's Defence Weekly**, August 13, 1997, v. 28, no. 6, p. 29-30.

Cook, Nick, et al. "Scenario 2015: How Science Shapes War." **Jane's Defence Weekly**, June 11, 1997, v. 27, no. 23, p. 47+

Cooper, Pat. "C3I (Command, Control, Communications, and Intelligence), Data Becomes Battlefield Targets." **Defense News**, December 4-10, 1995, v. 10, p. 8, 42.

_____. "DOD Directive Links Into War Intelligence, Operations: Updated Policy Will Provide Clearer Picture of Roles." **Defense News**, October 14-20, 1996, v. 11, p. 84.

_____. "Evolving IW Faces Established Military Doctrine." **Defense News**, December 4-10, 1995, v. 10, p. 10.

_____. "In Cyberspace, U.S. Confronts an Illusive Foe." **Defense News**, February 13-19, 1995, v. 10, p. 1+

_____. "Information Laboratory Would Link C4 Efforts." **Defense News**, December 18-24, 1995, v. 10, p. 3+

_____. "Information Warfare." **Defense News**, December 4-10, 1995, v. 10, p. 8-16.

_____. "Information Warfare Sparks Security Affairs Revolution." **Defense News**, June 16, 1995, v. 10, p. 1+

_____. "Navy Battles Computer Threats: Opens School to Teach Information Warfare Tactics, Doctrine." **Defense News**, October 30 – November 5, 1995, v. 10, p. 4+

_____. "Pentagon Debates Potential of Information Warfare." **Defense News**, May 13-19, 1996, v. 11, p. 3+

Cooper, Pat and Jason Glashow. "New Army Doctrine Shaped by Info Warfare." **Army Times**, January 15, 1996, v. 56, no. 25, p. 11.

Cooper, Pat, and Robert Holzer. "America Lacks Reaction Plan for Info War." **Defense News**, October 2-8 1995, v. 10, p. 3+

_____. "Pentagon Rethinks Art of War: Studies New Role for Information Warfare." **Defense News**, February 20-26, 1995, v. 10, p. 3+

_____. "U.S. Navy Stresses IW Training at New Facility." **Defense News**, December 4-10, 1995, v. 10, p. 14.

Cooper, Pat and Frank Oliveri. "Air Force Carves Operations Edge in Info Warfare." **Defense News**, August 21-27, 1995, v. 10, p. 1+

_____. “Hacker Exposes U.S. Vulnerability.” **Defense News**, October 9-15, 1995, v. 10, p. 1+

Copley, Gregory R. “Re-Defining Psychological Strategy in the Age of Information Warfare.” **Defense & Foreign Affairs Strategic Policy**, June 1998, v. 26, no. 6, p. 5-8.

Corcoran, Michael J. “Information Warfare and Defending the UK Nation State.” **Computers & Security**, 1997, v. 16, no. 6, p. 525.

Corless, Josh. “Hunting Goliath in the Age of Asymmetric Warfare.” **Jane's Navy International**, December 1, 1999, v. 104, no. 10, p. 23-26.

Cormier, Ken. “I2WD Completes Relocation to CECOM Headquarters at Ft. Monmouth.” **Journal of Electronic Defense**, January 1998, v. 21, no. 1, p. 26-27.

Coroalles, Anthony M. “On War in the Information Age: A Conversation with Carl Von Clausewitz.” **Army**, May 1996, v. 46, no. 5, p. 24-26+.

_____. “On War in the Information Age: A Conversation with Carl Von Clausewitz.” **Army**, May 1996, v. 46, no. 5, p. 24-26+

Correll, John T. "Warfare in the Information Age." Editorial. **Air Force Magazine**, December 1996, v. 79, no. 12, p. 3.

Crilley, Kathy. “Information Warfare: New Battlefields Terrorists, Propaganda and the Internet.” **ASLIB Proceedings**, July/August 2001, v. 53, no. 7, p. 250-264.

Critchlow, Robert D. “Whom the Gods Would Destroy: An Information Warfare Alternative for Deterrence and Compellence.” **Naval War College Review**, Summer 2000, v. 53, no. 3, p. 21-38.

Croft, Michael. “Information Warfare: Media-Military Relations in Canada.” **Canadian Defence Quarterly**, Summer 1998, v. 27, no. 4, p. 34-35.

Cronin, Blaise. “Information Warfare: Peering Inside Pandora’s Postmodern Box.” **Library Review**, 2001, v. 50, no. 5/6, p. 279-294.

Cronin, Blaise and Holly Crawford. “Information Warfare: Its Application in Military and Civilian Contexts.” **Information Society**, October-December 1999, v. 15, no. 4, p. 257-263.

_____. “Raising the Intelligence Stakes: Corporate Information Warfare and Strategic Surprise.” **Competitive Intelligence Review**, 3rd Quarter 1999, v. 10, no. 3, p. 58-66.

Cross, Michael. “Threat of Cyber Sabotage Increases.” **Computer & Security**, 1999, v. 18, no. 5, p. 434-435.

Crowell, William P. “Security: Surfing Society’s Third Wave.” **Defense**, 1997, no. 2, p. 32-35.

“Crucial Network Imperatives Spawn Information War Peril.” **Signal**, June 1996, v. 50, no. 10, p. 35-38.

Curtis, Ian G.S. “Misinformed About Information War? The Three-Wave Theory is Under Fire.” **Defense & Foreign Affairs Strategic Policy,** March 1996, v. 24, no. 3, p. 4-5.

Curts, Raymond J. and Douglas E. Campbell. “The Impact of Architecture and Interoperability on Information Warfare Systems.” **Journal of Information Warfare**, 2001, v. 1, no. 1, p. 33-41.

Czerwinski, Thomas J. “Command and Control at the Crossroads.” **Parameters**, Autumn 1996, v. 26, no. 3, p. 121-132.
http://carlisle-www.army.mil/usawc/Parameters/96autumn/czerwins.htm

_____. “The Third Wave: What the Tofflers Never Told You.” **Strategic Forum**, April 1996, no. 72.
http://www.ndu.edu/inss/strforum/SF_72/forum72.html

Dahl, Erik J. “We Don't Need an IW (Information Warfare) Commander.” **United States Naval Institute Proceedings**, January 1999, v. 125, no. 1, p. 48-49.

Dark, Ken. “Information Warfare and Global Economic Security.” **Defence Systems International: The International Review of Land, Sea and Air Systems**, Autumn 1997, p. 111-113.

Darnton, Geoffrey. “Content Analysis as a Tool of Information Warfare.” **Journal of Information Warfare**, September 2005, v. 4, no. 2, p. 1-11.

_____. “Information Warfare, Revolutions in Military Affairs, and International Law.” **Journal of Information Warfare**, March 2005, v. 4, no. 1, p. 1-20.

Davis, John W. "Open Source Information." **Army**, July 1997, v. 47, no. 7, p. 7-9.

Davis, Norman C. "An Information-Based Revolution in Military Affairs," **Strategic Review**, Winter 1996, v. 24, no. 1, p. 43-53.

de Amarante, Albano and Jose Carlos. “The Automated Battle: A Feasible Dream?” **Military Review**, May 1994, v. 74, no. 5, p. 58-61.

Dearth, Douglas H. “Information War: Rethinking the Application of Power in the 21st Century.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 11-16.

Debban, Alan W. “Disabling Systems: War-Fighting Option for the Future.” **Airpower Journal**, Spring 1993, v. 7, no. 1, p. 44-50.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj93/spr93/debban.htm

“Defense Department's Achilles' Heel Targeted for Heightened Protection.” **Signal**, July 1999, v. 53, no. 11, p. 57-59.

DeGroat, Arthur S. and David C. Nilsen, "Information and Combat Power on the Force XXI Battlefield," **Military Review**, November-December 1995, v. 75, no. 6, p. 56-62.

DeGroat, Arthur S. and Michael J. Stagoski. “Mounted Battle Command in the Information Age.” **Army**, September 1994, v. 44, no. 9, p. 10+

Deitchman, S.J. “Information Warfare. “ **Issues in Science and Technology**, Winter 1995-1996, v. 12, no. 2, p. 15-17.

Devereaux, Christopher. "Combat Leadership and the Media." **United States Naval Institute Proceedings**, July 1995, v. 121, no .7, p. 62-65.

Devost, M, B. Houghton and N. Pollard. “Information Terrorism: Political Violence in the Information Age.” **Terrorism and Political Violence**, Spring 1997, v. 9, no. 1, p. 72-83.

Dezhin, E.N. “Information Warfare as Chinese Analysts See It.” **Military Thought**, 1999, v. 9, no. 6, p. 82-85.

DiCenso, David J. “IW Cyberlaw: The Legal Issues of Information Warfare.” **Law Technology**, 2nd Quarter 2000, v. 33, no 2, p. 1-25.

Dick, Charles. “Russian Views on Future War – Part One.” **Jane’s Intelligence Review**, September 1993, v. 5, no. 9, p. 390-392.

_____. “Russian Views on Future War – Part Two.” **Jane’s Intelligence Review**, October 1993, v. 5, no. 10, p. 451-453.

_____. “Russian Views on Future War – Part Three.” **Jane’s Intelligence Review**, November 1993, v. 5, no. 11, p. 488-495.

Dietz, Lawrence D. “Information Warfare Poses New Threats: Are You Ready?” **Internet Security Advisor**, March/April 2000, v.3, no. 2, p. 8-10.

“Digital Formats Complicate Information Security Tasks.” **Signal**, February 1997, v. 51, no. 6, p. 21-23.

DiNardo, R.L. and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." **Airpower Journal**, Winter, 1995, v. 9, no. 4, p. 69-79. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/win95_files/dinardo.pdf*

Dockery, John. "C3: Information Science in Uniform." **Biosystems**, 1996, v. 38, no. 2-3, p. 253-257.

Dornheim, Michael A. “Bombs Still Beat Bytes.” **Aviation Week & Space Technology**, January 19, 1998, v. 148, no. 3, p. 60.

“DSB Warns US in Jeopardy from Information Warfare Threat.” **Journal of Electronic Defense**, February 1997, v. 20, no. 2, p. 15.

Echevarria, Antulio J, II. “Tomorrow's Army: The Challenge of Nonlinear Change.” **Parameters**, Autumn 1998, v. 28, no. 3, p. 85-98. *http://carlisle-www.army.mil/usawc/Parameters/98autumn/echevarr.htm*

Echevarria, Antulio and John M. Shaw. “The New Military Revolution: Post-Industrial Change.” **Parameters**, Winter 1992-1993, v. 22, no. 4, p. 70-79.

Eden, Steven J. ”Knowledge-Based Warfare Implications.” **Military Review**, March-April 1997, v. 77, no. 2, p. 49-51.

Edmiston, James P. “Changing the Face of War.” **INSCOM Journal**, March-April 1997, v. 20, no. 2, p. 12-17.

Edmonds, Albert J. “C4IFTW (Command, Control, Communications, Computers and Intelligence for the Warrior): Teamwork for the Warrior.” **Defense**, 1997, no. 2, p. 22-31.

Edwards, Sean J. A. “The Threat of High Altitude Electromagnetic Pulse to Force XXI.” **National Security Studies Quarterly**, Autumn 1997, v. 3, no. 4, p. 61-80.

Ehlers, Vernon J. “Information Warfare and International Security.” **The Officer (ROA National Security Report)**, September 1999, v. 75, no. 8, p. 28-32.

Emmett, Peter C. “Information Mania--a New Manifestation of Gulf War Syndrome?” **RUSI Journal**, February 1996, v. 141, no. 1, p. 19-26.

_____. “Software Warfare: The Emerging Future.” **RUSI Journal**, December 1992, v. 137, no. 6, p. 56-60.

_____. “Software Warfare: The Militarization of Logic.” **Joint Force Quarterly**, Summer 1994, no. 5, p. 84-90. *http://www.dtic.mil/doctrine/jel/jfq_pubs/jfq1405.pdf*

Eriksson, E. Anders. “Information Warfare: Hype or Reality.” **The Nonproliferation Review**, Spring/Summer 1999, v. 6, no. 3, p.57-64.

Essig, Christopher G. “The Information Revolution and International Security.” **Security Management**, September 1999, v. 43, no. 9, p. 194-196.

“Europe Seeks Overarching View of Information War.” **Signal**, July 1998, v. 52, no. 11, p. 33-35.

Evancoe, Paul. “Tomorrow’s Weapons of Choice.” **Military Technology**, June 1994, v. 18, no. 6, p. 68-71.

Evancoe, Paul R. and Mark Bentley. “Computer Viruses Loom as Future Era Weapons.” **National Defense**, February 1994, v. 78, no. 495, p. 19+

_____. “CVW -- Computer Virus as a Weapon.” **Military Technology**, May 1994, v. 18, no. 5, p. 38-40.

Evers, Stacey. "Joint Warrior Brings Combined Ops Closer." **Jane’s Defence Weekly**, April 2, 1997, v. 27, no. 13, p. 25+

_____. “Special Report: Information Warfare: Stop the Hacking of Cyber Information.” **Jane’s Defence Weekly**, April 10, 1996, v. 25, no. 15, p. 22-25.

_____. “Sweden Moves to Tighten up Security.” **Jane’s Defence Weekly**, November 12, 1997, v. 28, no. 19, p. 61.

_____. “US Navy Commissions New Information Centre.” **Jane’s Defence Weekly**, November 4, 1995, v. 24, no. 18, p. 11.

_____. "USA Aims to Improve Intelligence Security." **Jane’s Defence Weekly**, June 25, 1997, v. 27, no. 25, p. 27.

Evers, Stacey and Rupert Pengelley. "Warriors Break Down Firewalls with JWID (Joint Warrior Interoperability Demonstration)." **Jane’s Defence Weekly,** August 20, 1997, v. 28, no. 7, p. 25-26.

“EW Expands into Information Warfare.” **Aviation Week & Space Technology**, October 10, 1994, v. 141, no. 15, p. 47-48.

“Experts Focus on Reining in Information Technologies.” **Signal**, July 1999, v. 53, no. 11, p. 68-71.

Farris, Kate. “Chinese Views on Information Warfare.” **Defense Intelligence Journal**, Winter 2001, v. 10, no. 1, p. 37-58.

Fecci, Jo Marie. "Winning Hearts and Minds--Haitian Style." **VFW, Veterans of Foreign Wars Magazine**, February 1995, v. 82, no. 6, p. 32.

Felker, Edward J. “Information Warfare: A View of the Future.” **A Common Perspective**, September 1995, v. 3, no. 2, p. 17-18.
http://www.dtic.mil/doctrine/jel/comm_per/acp3_2.pdf

Ferguson, Michael G. “Internet: Our Enemy's Best Friend.” **Marine Corps Gazette**, January 1999, v. 83, no. 1, p. 48-50.

FitzGerald, Mary C. "The Russian Military’s Strategy for ‘Sixth Generation’ Warfare." **Orbis**, Summer 1994, v. 38, no. 3, p. 457-476.

_____. "Russian Views on Electronic Signals and Information Warfare." **American Intelligence Journal**, Spring/Summer 1994, v. 15, no. 1, p. 81-87.

_____. "Russian Views on Information Warfare." **Army**, May 1994, v. 44, no. 5, p. 57-58+

FitzSimonds, James R. “Cultural Challenge of Information Technology.” **Naval War College Review**, Summer 1998, v. 51, no. 3, p. 9-21.

FitzSimonds, James R. and Jan M. Van Tol. “Revolutions in Military Affairs.” **Joint Force Quarterly**, Spring 1994, no. 4, p. 24-31.
http://www.dtic.mil/doctrine/jel/jfq_pubs/jfq0604.pdf

Flaherty, Christopher. “Information Warfare and Mimicking Operations.” **Australian Army Journal**, December 2003, v. 1, no. 2, p. 11-14.
http://www.defence.gov.au/army/lwsc/AbstractsOnline/AAJournal/2004_S/AAJ_s_2003_01.pdf

Flaver, Peter D “Blowback: Information Warfare and the Dynamics of Coercion.” **Security Studies**, Summer 1998, v. 7, no. 4, p. 88-120.

Flynt, Bill. “Threat Convergence.” **Military Review**, September/October 1999, v. 79, no. 5, p. 2-11.

Fogleman, Ronald R. "What Information Warfare Means to You." **Air Force Times**, July 17, 1995, v. 55, no. 50, p. 31.

Forster, Anthony. “On Hackers, Crackers and Phreakers.” **Jane's Intelligence Review**, January 1999, v. 11, no. 1, p. 50-54.

Fowler, Bruce W. and Donald R. Peterson. “Information Age Warfare.” **OR/MS Today**, April 1997, v. 24, no. 2, p. 34-37.

Fox, Robert. “Information Warfare…” **Communications of the ACM**, August 1996, v. 39, no. 8, p. 12.

Franks, Fredrick M., Jr. “Winning the Information War: Evolution and Revolution.” **Vital Speeches of the Day**, May 15, 1994, v. 60, no. 15, p. 453-458.

Freakley, Benjamin C. “Information Warfare: The Next Dimension.” **Infantry**, September-October 2004, v. 93, no. 5, p. 1-2.

Fredericks, Brian E. "Information Warfare at the Crossroads." **Joint Force Quarterly**, Summer 1997, no. 16, p. 97-103.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1816pgs.pdf

Freedman, Lawrence. “The Changing Forms of Military Conflict. “ **Survival**, Winter 1998-1999, v. 40, no. 4, p. 39-56.

Friedman, Norman. “Information Warfare Can Defeat Terrorists.” **US Naval Institute Proceedings**, April 2003, v. 129, no. 4, p. 4+

Friman, Henrik. “A Systems View of Information Warfare.” **Journal of Information Warfare**, 2001, v. 1, no. 1, p. 25-32.

Fulghum, David A. "ACC Weighs Plans for New Technology But Plans to Keep USAF's Strike Arm Honed For Emerging Threats Regularly Pit Budget Cuts Against the Need to Modernize and Maintain Operational Flexibility." **Aviation Week & Space Technology**, April 29, 1996, v. 144, no. 18, p. 38+

_____. “Compass Call to Dominate Electronic, Info Warfare Military Reliance on Rapid, Uninterrupted Communications for Survival has Made Data Flow a Major Focus of Attack.” **Aviation Week & Space Technology**, October 18, 1999, v. 151, no. 16, p. 50+

_____. “Computer Warfare Offense Takes Wing.” **Aviation Week & Space Technology**, January 19, 1998, v. 148, no. 3, p. 56-58.

_____. “Info War Fleet Tapped for Fast Deployment.” **Aviation Week & Space Technology**, February 9, 1998, v. 148, no. 6, p. 90-91.

_____. “New Weapons Slowed by Secrecy Clampdown.” **Aviation Week & Space Technology**, January 19, 1998, v. 148, no. 3, p. 54-56.

_____. “Telecom Links Provide Cyber-Attack Route.” **Aviation Week & Space Technology**, November 8, 1999, v. 151, no. 19, p. 81-83.

_____. “Two-War Strategy May be Abandoned.” **Aviation Week & Space Technology**, January 29, 1996, v. 144, no. 5, p. 40+

_____. “Yugoslavia Successfully Attacked by Computers.” **Aviation Week & Space Technology**, August 23, 1999, v. 151, no. 8, p. 31+

Furnell, S. M. and M. J. Warren. “Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?” **Computers & Security**, 1999, v. 18, no. 1, p. 28-34.

Gallogly-Staver, Erin J. and Raymond S. Hilliard. “Information Warfare: OPFOR Doctrine – An Integrated Approach.” **Military Intelligence Professional Bulletin**, July-September 1997, v. 23, no. 3, p. 53-55 and **News From the Front!**, September/October 1997, p. 12-18.

Gambel, Daniel W. "MLS (Multi-Level Security): Data Security for the DOD and the Rest of Us." **Defense Electronics**, June 1995, v. 27, no. 6, p. 10+

Garber, Lee. “DoD Discusses Information Warfare.” **Computer**, March 197, v. 30, no. 3, p. 18+

Garrett, Stephen F. “Evolving Information-Age Battle Staffs.” **Military Review**, March-April 1998, v. 78, no. 2, p. 28-36.

Gehly, Darryl. “Controlling the Battlefield.” **Journal of Electronic Defense**, June 1993, v. 16, no, 6, p. 42-49.

Gelbach, Douglas K. “Extending the Littoral Battlespace.” **Marine Corps Gazette**, October 1998, v. 82, no. 10, p. 23-24.

Gellman, Robert. “Who’s the Victor in Information Warfare?” **Government Computer News**, August 21, 1995, v. 14, no. 17, p. 26.

Gentry, John A. “Knowledge-Based Warfare: Lessons from Bosnia.” **The Officer** (**ROA Security National Report)**, January/February 1999, v. 75, no. 1, p. 137-142.

Giboney, Thomas B. “Commander’s Control from Information Chaos.” **Military Review**, November 1991, v. 71, no. 11, p. 34-38.

Glashow, Jason. “Army to Focus on System Resistance to Infiltration: Heavy Science Reliance on Computers Creates New Openings for Foes.” **Defense News**, December 4-10, 1995, v. 10, p. 16.

“Global Intelligence: the Web Expands.” **Jane's International Defense Review**, April 1997, v. 2, no. 4, p. 5.

Goldman, Alan R. and Eric Vardac. “Threats to the New World Order.” **Military Intelligence Professional Bulletin**, January-March 1994, v. 19, no. 1, p. 42-46.

Gompert, David C. "National Security in the Information Age." **Naval War College Review**, Autumn 1998, v. 51, no. 4, p. 22-41.

Goodman, Glenn W., Jr. "Power of Information: Air Force Clarifies Its Misunderstood Virtual Presence Concept." **Armed Forces Journal International**, July 1995, v. 132, no. 12, p. 24.

Goodman, Sy E. “War, Information Technologies, and International Asymmetries.” **Communications of the ACM**, December 1996, v. 39, no. 12, p. 11-15.

Goodwin, Brent Stuart. “Don’t Techno for an Answer: The False Promise of Information Warfare.” **Naval War College Review**, Spring 2000, v. 53, no. 2, p. 215-224.

Gourley, Robert D. "The Devil is in the Details." **United States Naval Institute Proceedings**, September 1997, v. 123, no. 9, p. 86-88.

Gray, Colin S. “Changing Nature of Warfare?” **Naval War College Review**, Spring 1996, v. 49, no. 2, p. 7-22.

Gray, Jim. “Turning Lessons Learned into Policy.” **Journal of Electronic Defense**, October 1993, v. 16, no. 10, p. 87-92.

Green, Gerald. "DSB Warns US in Jeopardy from Information Warfare Threat." **Journal of Electronic Defense**, February 1997, v. 20, no. 2, p. 15.

_____. “Self-Inflicted Information Warfare? The ‘Year 2000 Problem.’” **Journal of Electronic Defense**, April 1998, v. 21, no. 4, p. 17-18.

Gregory, Thomas E. "Cybernetic Design: Maneuver Warfare Organization for the Information Age." **Marine Corps Gazette**, December 1994, v. 78, no. 12, p. 38-40.

Grier, Peter. "At War with Sweepers, Sniffers, Trapdoors, and Worms." **Air Force Magazine**, March 1997, v. 80, no. 3, p. 20-24.

Grier, Peter. “The Data Weapon.” **Government Executive**, June 1992, v. 24, no. 6, p. 20+

_____. “Preparing for 21st Century Information War.” **Government Executive**, August 1995, v. 27, no. 8, p. 130+

_____. "From the Battlelabs.” **Air Force Magazine**, September 1998, v. 81, no. 9, p. 48-50.

_____. "Information Warfare." **Air Force Magazine**, March 1995, v. 78, no. 3, p. 34-37.

Griffin, Gary B. “Future Foes, Future Fights.” **Military Review**, November 1994, v. 74, no. 11, p. 56-60.

Grimes, Vincent P. "Digitized Zephyr Lifting Fog from No Man's Land: Army Pushes Information Warfare Transition." **National Defense,** September 1995, v. 80, no. 510, p. 32-33.

Grohoski, David C. Steven M. Seybert and Marc J. Romanych. “Measures of Effectiveness in the Information Environment.” **Military Intelligence Professional Bulletin**, July-September 2003, v. 29, no. 3, p. 12-16. *http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=267&issueID=19*

Guenther, Otto and Robert F. Giordano. “Enabling Technologies and Advanced Concepts for the Digitized Force XXI.” **Army RD&A**, November 1994, no. 6, p. 21-24.

Guilbault, R.G. "Information Empowerment: The Key Force Multiplier." **Defense & Security Electronics**, January 1996, v. 28, no. 1, p. 10+

Gumadad, Arsemio T, II. "Profession of Arms in the Information Age." **Joint Force Quarterly**, Spring 1997, no. 15, p. 14-20. *http://www.dtic.mil/doctrine/jel/jfq_pubs/06_15.pdf*

Haeni, Reto. “Information Warfare: An Introduction.” **Soldier-Scholar**, Fall 1996, v. 3, no. 3, p. 3-10.

Haertling, Kenneth P., et al. “Implementing Information Warfare in the Weapon Targeting Process.” **Military Operations Research**, 1999, v. 4, no. 1, p. 57-65.

Haibeck, Kevin S. "IPB (Intelligence Preparation of the Battlefield) in the Third Dimension **Military Intelligence Professional Bulletin**, July-September 1990, v. 16, no. 3, p. 36-37.

Hammes, Thomas X. “Don't Look Back, They're not Behind You.” **Marine Corps Gazette**, May 1996, v. 80, no. 5, p. 72.

_____. "Evolution of War: The Fourth Generation." **Marine Corps Gazette**, September 1994, v. 78, no. 9, p. 35-38+

_____. “War Isn't a Rational Business.” **United States Naval Institute Proceedings**, July 1998, v. 124, no. 7, p. 22-25.

Hammond, James W., III. “Electronic Attack: Key to Our Future.” **Marine Corps Gazette**, December 1999, v. 83, no. 12, p. 30-32.

Hancock, Bill. “Information Warfare: The Next Front.” **Computers & Security**, 1999, v. 18, no. 2, p. 101-102.

_____. “Information Warfare Highlighted as a Concern by US Government.” **Computers & Security**, 2001, v. 20, no. 1, p. 8-9.

Hankins, Michelle L. “Defense Department's Achilles' Heel Targeted for Heightened Protection.” **Signal**, July 1999, v. 53, no. 11, p. 57-59.

_____. “Social, Criminal Protagonists Engage in New Information Age Battle Techniques.” **Signal**, July 1999, v. 53, no. 11, p. 53-54.

Hardy, Stephen M. "Accessing the Digital Battlefield." **Journal of Electronic Defense**, January 1994, v. 17, no. 1, p. 31+

_____. "The New Guerrilla Warfare (Protecting DOD Computer and Communications Assets)." **Journal of Electronic Defense**, September 1996, v. 19, no. 9, p. 46-52.

_____. "A Question of Symmetry?" **Journal of Electronic Defense**, January 1997, v. 20. no. 1, p. 42-44+

_____. "Should We Fear the Byte Bomb?" **Journal of Electronic Defense**, January 1996, v. 19, no. 1, p. 42-48.

Harig, Paul T. “The Digital General: Reflections in Leadership in the Post-Information Age.” **Parameters**, Autumn 1996, v. 26, no. 3, p. 133-140.
http://carlisle-www.army.mil/usawc/Parameters/96autumn/harig.htm

Harknett, Richard J. "Information Warfare and Deterrence." **Parameters**, Autumn 1996, v. 26, no. 3, p. 93-107.
http://carlisle-www.army.mil/usawc/Parameters/96autumn/harknett.htm

Harley, Jeffrey A. “Information, Technology, and the Center of Gravity.” **Naval War College Review**, Winter 1997, v. 50, no. 1, p. 66-87.

Haslam, Emily. “Information Warfare: Technological Changes and International Law.” **Journal of Conflict and Security Law**, 2000, v. 5, no. 2, p. 157-175.

Hayes, Richard E. and Gary Wheatley. "Information Warfare and Deterrence." **Strategic Forum**, no. 87, October 1996, no. 87.
http://www.ndu.edu/inss/strforum/SF_87/forum87.html

Henry, Ryan and C. Edward Peartree. “Assessing 'Byte City': An Insightful or Misleading Vision?” **Washington Quarterly**, Spring 1997, v. 20, no. 2, p. 73-78.

_____. “Military Theory and Information Warfare.” **Parameters**, Autumn 1998, v. 28, no. 3, p. 121-135.
http://carlisle-www.army.mil/usawc/Parameters/98autumn/henry.htm

Herd, Graeme P. “The Russo-Chechen Information Warfare and 9/11: Al-Qaeda Through the South Caucasus Looking Glass?” **European Security**, Winter 2002, v, 11, no. 4, p. 110-130.

Herman, Mark. “Entropy-Based Warfare: Modeling the Revolution in Military Affairs.” **Joint Force Quarterly**, Autumn/Winter 1998-1999, no. 20, p. 85-90. *http://www.dtic.mil/doctrine/jel/jfq_pubs/1620.pdf*

Hill, Martin R. “It Is Time to Get on With Information Warfare.” **Defense Intelligence Journal**, Spring 1996, v. 5, no.1, p. 25-41.

Hinde, Stephen. “Cyber Wars and Others Threats.” **Computer & Security**, March 1998, v. 17, no. 2, p. 115-118.

Hobby, Jason. “Cyber Leeches.” **Computer Weekly**, December 5, 1996, p. 46+

Holinko, Myron. “Use of the Digital Integrated Lab for Force XXI.” **Army RD&A**, March-April 1996, p. 9-12.

Holzer, Robert. “Rapid Dominance Concept Aims to Stun Enemy Forces: ‘Bedlam Brigades' Would Inject Widespread Chaos.” **Army Times**, September 28, 1998, v. 59, no. 9, p. 24.

_____. “U.S. Navy Begins Information War Effort.” **Defense News**, August 29-September 4, 1994, v. 9, p. 4.

Houghtaling, Pamela A. “New Information Warfare System Advances Army into Next Century.” **Signal**, March 1996, v. 50, no. 7, p. 37-39.

Hubbard, Zachary P. “Information Warfare in Kosovo.” **Journal of Electronic Defense**, November 1999, v. 22, no. 11, p. 57-60.

Hudgins-Bonafield, Christy. “Tackling Network Security Can Be An Uphill Battle.” **Computers & Security**, 1997, v. 16, no. 3, p. 217.

Hughes, David. "609th Sqdn. Pursues New Realm of Combat." **Aviation Week & Space Technology**, April 29, 1996, v. 144, no. 18, p. 52-53.

_____. "Cyber Raid, Wall Street: This is No Drill. . . ." **Aviation Week & Space Technology**, December 29, 1997, v. 147, no. 25/26, p. 98.

Hunt, Carl W. "Commercial Systems Enhance Information Warfare Capability." **Signal**, March 1997, v. 51, no. 7, p. 64-65.

Hunter, Roger C. "Disabling Systems and the Air Force." **Airpower Journal**, Fall 1994, v. 8, no. 3, p. 43-47.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj94/fal94/hunter.html

Hurst, Elizabeth. “Introduction to Command and Control Warfare.” **Cyber Sword**, Spring 1997, v. 1, no. 1, p. 10-14.

_____. “What is C2W?” **Cyber Sword**, Fall 1997, v. 1, no. 2, p. 18-25.

Hutchison, Katherine K. “Firewalls Offer Capable Internet Security Links: Avoiding a Mugging in Cyberspace Requires Dedicated Security System.” **National Defense**, July-August 1995, v. 80, p. 58-60.

Hutchinson, William. “Concepts in Information Warfare.” **Logistics Information Management**, 2002, v. 15, no. 5/6, p. 410-413.

_____. “Information Warfare and Deception.” **Informing Science**, 2006, v. 9, no. 9, p. 213-223.
http://inform.nu/Articles/Vol9/v9p213-223Hutchinson64.pdf

Hutchinson, William and Matt Warren. “Principles of Information Warfare.” **Journal of Information Warfare**, 2001, v. 1, no. 1, p. 1-6.

Koacich, Gerald L. and Andy Jones. “What InfoSec Professionals Should Know About Information Warfare Tactics by Terrorists.” **Computers & Security**, 2002, v. 21, no. 1, 35-40.

"Industry, Government Pursue Data Security Clearinghouse." **Signal**, March 1997, v. 51, no. 7, p. 69-71.

"Information Afterburners Boost Aerial Operations." **Signal**, November 1996, v. 51, no. 3, p. 31-33.

“Information and Command and Control.” **Aerospace America**, December 1999, v. 37, no. 12, p. 32+

"Information Officers Disseminate, Protect Intelligence Agency Data." **Signal**, July 1997, v. 51, no. 11, p. 59-62.

“Information Systems, Networks Spark Major Security Challenges.” **Signal**, June 1996, v. 50, no. 10, p. 43.

“Information Warfare.” **Defense Intelligence Journal**, Spring 1996, v. 5, no.1, entire issue.

“Information Warfare.” **Secure Computers and Networks**, Spring 2000, p. 329-344.

"Information Warfare Center." **Security**, 1996, v. 33, no. 1, p. 10+

“Information Warfare Battlelab Stands Up.” **Airman**, May 1997, v. 41, no. 5, p. 10.

“Information Warfare, Cyberterrorism and Information Assurance.” **Communication Booknotes**, May/June 1997, v. 28, no. 3, p. 38-39.

“Information Warfare: A Sneak Attack on America's Computer Infrastructure Could Bring the Country to Its Knees in Less Than an Hour. So Will the United States Strike First?” **Popular Mechanics**, March 1999, v. 173, no. 3, p. 58-61.

"Information Warriors Raze Enemy's Vital Data Chains." **National Defense**, March 1995, v. 79, no. 506, p. 30-31.

“Information Warfare – Something New, Something Borrowed, Something Old?” **Computer Fraud & Security**, 2000, v. 1999, no. 10, p. 16-18.

"Integration Efforts Mold Information Technology." **National Defense**, October 1994, v. 79, no. 501, p 24+

“Is the Virus Threat Under Control?” **Computer Security Journal**, 1996, v. 12, no.1, p. 57-66.

Issler, Gordon D. “Space Warfare Meets Information Warfare.” **Joint Force Quarterly**, Autumn 2000, no. 26, p. 100-104.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1926.pdf

“IT Security: What You Don't Know Can Hurt You.” **Chief Executive**, April 1998, no. 133, p. 10-11.

Jajodia, Sushil, et al. “Surviving Information Warfare Attacks.” **Computer**, April 1999, v. 32, no. 4, p. 57-63.

Jensen, Owen E. "Information Warfare: Principles of Third-Wave War." **Airpower Journal**, Winter 1994, v. 8, no. 4, p. 35-43.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj94/win94/jenson.html

Johnson, Collie J. “NDIA (National Defense Industrial Association) 15th Annual T&E (Test and Evaluation) Conference Draws Large, Diverse Crowd--Translating Data into Information into Knowledge into Understanding into Combat Decisions.” **Program Manager**, May-June 1999, v. 28, no. 3, p. 44-50.
http://www.dau.mil/pubs/pm/pmpdf99/jhnsn2mj.pdf

Johnson, Craig L. "Information Warfare--Not a Paper War." **Journal of Electronic Defense**, August 1994, v. 17, no. 8, p. 55-56+

Johnson, Jeff. “The Military Impact of Information Technology.” **Communications of the ACM**, April 1997, v. 40, no. 4, p. 20-22.

Jones, Jeffery B. "Theater Information Strategies." **Military Review**, November 1994, v. 74, no. 11, p. 48-50.

Jones, Michael G. “Inside the Beltway Warfare Plans.” **Communications of the ACM**, March 1997, v. 40, no. 3, p. 27-28.

Jormakka, Jorma and J.V. W. Mölsä. “Modelling Information Warfare as a Game.” **Journal of Information Warfare**, September 2005, v. 4, no. 2, p. 12-25

Joyner, Christopher C. and Catherine Lotriont e. “Information Warfare as International Coercion: Elements of a Legal Framework.” **European Journal of International Law**, December 2001, v. 12, no. 5, p. 825-865.

Kabay, M. E. "Prepare Yourself for Information Warfare." **Computerworld**, March 20, 1995, v. 29, no. 12, p. S2+

Kabay, Michel. “Information Warfare Could be More Than Fiction.” **Network World**, September 6, 1993, v. 10, no. 36, p. 32+

Kagan, Frederick W. “Star Wars in Real Life: Political Limitations on Space Warfare.” **Parameters**, Autumn 1998, v. 28, no. 3, p. 112-120.
http://carlisle-www.army.mil/usawc/Parameters/98autumn/kagan.htm

Kaminski, Paul G. “Sustaining Flight Through Knowledge: Remarks at the Ira C. Eaker Distinguished Lecture on National Defense Policy, U.S. Air Force Academy, Colorado Springs, Colo., May 2, 1996.” **Defense Issues**, 1996, v. 11, no. 42, p.1-4.
http://www.defenselink.mil/speeches/speech.aspx?speechid=963

Kaplan, Ray. “It’s the Infrastructure, Stupid.” **Computer & Security**, 1996, v. 15, no. 5, p. 413.

Kendall, Frank. “Exploiting the Military Technical Revolution: A Concept for Joint Warfare.” **Strategic Review**, Spring 1992, v. 24, no. 2, p. 23-30.

Kennedy, Fred, et al. “Failure of Vision: Retrospective.” **Airpower Journal**, Summer 1998, v. 12, no. 2, p. 84-94.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj98/sum98/kennedy.html OR
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj98/sum98/kennedy.pdf

Kennedy, Harold. “Defense Data ‘Jewels' to Remain Vulnerable.” **National Defense**, July-August 1999, v. 83, no. 549, p. 50-51+

Kipp, Jacob W. "Confronting the RMA (Revolution in Military Affairs) in Russia. " **Military Review**, May-June 1997, v. 77, no. 3, p. 49-55.

Kiras, James. "Information Warfare and the Face of Conflict in the Twenty-First Century." **Peacekeeping & International Relations**, July/August 1996, v. 25, no. 4, p. 8-10.

_____ "Information Warfare and the Face of Conflict in the Twenty-First Century." **Soldier-Scholar**, Fall 1996, v. 3, no. 3, p. 40-42.

Kish, Steve C. "Do We Need an Information Warrior?" **Marine Corps Gazette**, January 1997, v. 81, no. 1, p. 20-22.

Kitfield, James. "Live by the Sword, Die by Software." **Government Executive**, November 1995, v. 27, no. 11, p. 72+

Knowles, John. “Eyes in the Sky.” **Journal of Electronic Defense**, August 1997, v. 20, no. 8, p. 37-38+

_____. “IW Battlelab to Go Operational This Month.” **Journal of Electronic Defense**, June 1997, v. 20, no. 6, p. 26+

Koch, Andrew. “USA to Form New Warfare Centre.” **Jane’s Defence Weekly**, October 13, 1999, v. 32, no. 15, p. 11.

Kojac, Jeffrey S. “Beyond C2: Dangers and Opportunities.” **Marine Corps Gazette**, October 1998, v. 82, no. 10, p. 37-39.

Komov, S. A. “Forms and Methods of Information Warfare.” **Military Thought**, 1997, v. 6, p. 22-26.

_____ “Information Warfare in Modern War: Theoretical Problems.” **Military Thought**, 1996, v. 5, p. 76-80.

Kopp, Carlo. “Shannon, Hypergames and Information Warfare.” **Journal of Information Warfare**, March 2003, v. 2, no. 2, p. 108-118.

Koretsky, Aleksandr. “Information Bomb Takes Nuclear Bomb's Place.” **The Current Digest of the Post - Soviet Press**, January 13, 1999, v. 50, no. 50, p. 20-21.

Kovacich, Gerald L. “Information Warfare and the Information Systems Security Professional.” **Computers & Security**, 1997, v. 16, no. 1, p. 14-24.

Kraus, George F., Jr. "Information Warfare in 2015." **United States Naval Institute Proceedings**, August 1995, v. 121, no. 8, p. 42-45.

Kreisher, Otto. “Next Steps in Information Warfare.” **Air Force Magazine**, June 1999, v. 82, no. 6, p. 52-55.

Krepinevich, Andrew F., Jr. “Recasting Military Roles and Missions.” **Issues in Science and Technology**, Spring 1995, v. 11, no. 3, p. 41-48.

Kruczek, Steven. “Zap!” **Harvard International Review**.” Winter 1997, v. 20, no. 1, p. 13-14.

Kuehl, Dan. "Defining Information Warfare." **Officer**, November 1997, v. 73, no. 11, p. 31-33. Also, **Strategic Forum**, June 1997, no. 115. *http://www.ndu.edu/inss/strforum/SF115/forum115.html*

_____. "Joint Information Warfare: An Information-Age Paradigm for Jointness." **Strategic Forum**, March 1997, no. 105. 4p. *http://www.ndu.edu/inss/strforum/SF105/forum105.html*

Kutner, Joshua A. "U.S. Success in Future Battlefield Hinges on Information Advantage." **National Defense**, December 1997, v. 82, no. 533, p. 24-25.

Lacey, James. “How Much Raw Data is Enough for Commanders in the Information Age?” **Army**, September 1999, v. 49, no. 9, p. 12-13.

Laos, Nicolas K. “Information Warfare and Low Intensity Operations.” **Perceptions**, June/August 1999, v. 4, no. 2, p. 174-195.

Latham, A. “The Contemporary Restructuring of the US Arms Industry: Toward Agile Manufacturing.” **Contemporary Security Policy**, April 1997, v. 18, no.1, p. 109-134.

Lawlor, Bruce M. "Information Corps: DOD Needs to Tap the Civilian Expertise Resident in its Reserve Components." **Armed Forces Journal International**, January 1998, v. 135, no. 6, p. 26-28.

Lawlor, Maryann. “Tenacious Security Vigilance Disarms Technology Terrorists.” **Signal**, July 1998, v. 52, no. 11, p. 37-39.

_____. "Science Board Task Force Challenges Defensive Information Warfare Status." **Signal,** September 1997, v. 52, no. 1, p. 63-66.

Leonhard, Robert R. “Shedding Light on the ‘Man in the Dark'.” **Army**, February 1997, v. 47, no. 2, p 40-42+

"Leveraging the Infosphere: Surveillance and Reconnaissance in 2020." **Airpower Journal**, Summer 1995, v. 9, no. 2, p. 8-25. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/sum95_files/spacast1.htm*

Levien, Fred. “Information Warfare: The Plain Truth.” **Journal of Electronic Defense**, April 1999, v. 22, no. 4, p. 47-53.

Levien, Frederic H. “Kosovo: An IW (Information Warfare) Report Card.” **Journal of Electronic Defense**, August 1999, v. 22, no. 8, p. 47-51.

Libicki, Martin. "The Emerging Primacy of Information." **Orbis**, Spring 1996, v. 40, no. 2, p. 261-276.

_____. "Information & Nuclear RMAs Compared." **Strategic Forum**, July 1996, no. 82.
http://www.ndu.edu/inss/strforum/SF_82/forum82.html

_____. “Information War, Information Peace.” **Journal of International Affairs**, Spring 1998, v. 51, no. 2, p. 411-428.

_____. “Information Warfare: A Brief Guide to Defense Preparedness.” **Physics Today**, September 1997, v. 50, no. 9, p. 40-45.

_____. “Rethinking War: the Mouse’s New Roar?” **Foreign Policy**, Winter 1999-2000, no. 117, p. 30-43.

_____. "What is Information Warfare?" **Strategic Forum**, May 1995, No. 28
http://www.ndu.edu/inss/strforum/SF_28/forum28.html

Libicki, Martin C. and James A. Hazlett. "Do We Need an Information Corps?" **Joint Force Quarterly**, Autumn 1993, no. 2, p. 88-97.
http://www.dtic.mil/doctrine/jel/jfq_pubs/jfq1302.pdf

Limno, A.N. and M. F. Krysanov. “Information Warfare and Camouflage, Concealment and Deception.” **Military Thought**, 2003, v. 12, no. 2, p. 181-185.

Lind, William S., et al. “The Changing Face of War into the Fourth Generation.” **Military Review**, October 1989. v. 69, no. 10, p. 2-11.

_____. “Fourth Generation Warfare: Another Look.” **Marine Corps Gazette**, December 1994, v. 78, no. 12, p. 34+

Lipinski, Tomas A. “Information Warfare, American Style.” **IEEE Technology and Society Magazine**, Spring 1999, v. 18, no. 1, p. 10-19.

Liu, Peng, Paul Ammann, Sushil Jojpdia. "Rewriting Histories: Recovering From Malicious Transactions." **Distributed and Parallel Databases**, 2000, v. 8, no. 1, p. 7-40.

Loescher, Michael S. “Moving the Navy into the Information Age.” **United States Naval Institute Proceedings**, January 1999, v. 125, no. 1, p. 40-44.

Longhouser, John E. “Converting Computing Power into Combat Power.” **Army RD&A**, March-April 1996, p. 4-8.

Lum, Zachary A. “Don't Slam It, Jam It! (Electronic/Information Warfare).” **Journal of Electronic Defense**, May 1996, v. 19, no. 5, p. 42+

_____. “Linking the Senses.” **Journal of Electronic Defense**, August 1994, v. 17, no. 8, p. 33-38.

_____. “Pump Up the Volume – Here Comes the Jam.” **Journal of Electronic Defense**, June 1994, v. 17, no. 6, p. 34+

_____. “We Want the Airwaves: Defense on the C2 (Command and Control) Front.” **Journal of Electronic Defense**, June 1996, v. 19, no. 6, p. 37-40.

Luzwick, Perry. “Maintaining a Competitive Advantage by Controlling Your Information Environment.” Part 1 of 4. **Computer Fraud & Security**, 2000, v. 2000, no. 1, p. 15-17.

_____. “On the Battlefield and in the Marketplace, Information is Much More Than Attacking Computer.” Part 2 of 4. **Computer Fraud & Security**, 2000, v. 2000, no. 2, p. 16-17.

Machlis, Sharon. “Security Experts: Hacker Detection is Key.” **Computerworld**, March 3, 1997, v. 31, no. 9, p. 59+

Madsen, Wayne. “CIA and NSA Sound Alarm Bells on INFOWAR.” **Computer Fraud & Security**, 1998, v. 1998, no. 8, p. 8-9.

_____. “Crypto Hacking and Infowar Squabbles.” **Computer Fraud & Security**, 1999, v. 1999, no. 1, p. 7-8.

_____. “Information Warfare: IT Security Professionals to Steer Clear.” **Computer Fraud & Security**, 2000, v. 2000, no. 2, p. 14-15.

_____. “Information Warfare: The Sequel.” **Computer Fraud & Security**, 1997, v. 1997, no. 2, p. 5-6.

_____. “Intelligence Agency Threats to Computer Security.” **International Journal of Intelligence and Counterintelligence**, Winter 1993, v. 6, no. 4, p. 413-488.

Mahanna, Cory W. and James Gagliarducci. "Army Aviation Bridges Communications on the Battlefield." **Military Review**, May-June 1995, v. 75, no. 3, p. 42-45.

Mahnken, Thomas G. "War in the Information Age." **Joint Force Quarterly**, Winter 1995-1996, no. 10, p. 39-43.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1110.pdf

Mains, Steven J. "Adopting Doctrine to Knowledge-Based Warfare." **Military Review**, March-April 1997, v. 77, no. 2, p. 93-95.

Malham, Mark C. and Debora Gabbard. “Battle Command Systems: The Force XXI Warfighter's Advantage.” **Military Review**, March-April 1998, v. 78, no. 2, p. 33-35.

Mann, Edward C. “Desert Storm: The First Information War?” **Airpower Journal**, Winter 1994, v. 8, no. 4, p. 4-14.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj94/win94/man1.html

Mann, Paul. “'Asymmetrical' Threats New Military Watchword.” **Aviation Week & Space Technology**, April 27, 1998, v. 148, no. 17, p. 55.

_____. “Pentagon Confronts Mounting Cyber Risks.” **Aviation Week & Space Technology**, March 22, 1999, v. 150, no. 12, p. 82-83.

_____. “Pentagon Flunks Cyber Defense [National Research Council Report on C4I Security Practices].” **Aviation Week & Space Technology**, April 19, 1999, v. 150, no. 15, p. 69-70.

_____. “Planning for the War of the Future.” **CQ Weekly**, Summer 1998, CQ Outlook Supplement, p. 18-19.

"Marine Corps Information Warfare Combines Services' Needs, Defines Their Differences." **Signal**, July 1996, v. 50, no. 11, p. 61-62.

Marsh, Robert T. “Securing, Protecting Critical U.S. Infrastructures.” **Defense Issues**, 1998, v. 13, no. 3, p. 1-6.

Martinez, Erasmo A. “Division XXI Intelligence Operations.” **Military Intelligence Professional Bulletin**, April-June 1996, v. 22, no. 2, p. 19-22.

Mason, Tony. “The Intelligence, Surveillance, Reconnaissance and Target Acquisition Requirement—an Overview.” **RUSI Journal**, December 1998, v. 143, no. 6, p. 55-59.

Matthews, William. "School is in for ‘Information Warfare' (School of Information Warfare and Strategy)." **Army Times**, May 23, 1994, v. 54, no. 43, p. 28.

_____. “Susceptible to Sabotage (Threat to Automated Information Systems).” **Air Force Times**, February 5, 1996, v. 56, no. 27, p. 28.

_____. “U.S. Army Tackles Data Vulnerability: Makes Plan to Assess Threats, Strengthen Electronic Security.” **Defense News**, February 5-11, 1996, v. 11, p. 38.

_____. “U.S. Forms Warfare School to Fight 'Information Overload.'” **Defense News**, May 16-22 1994, v. 9, p. 22.

Matthys, Erick T. "Harnessing Technology for the Future." **Military Review**, May-June 1995, v. 75, no. 3, p. 71-76.

Mazarr, Michael J. “Assessing ‘Byte City’: An Insightful or Misleading Vision?” **Washington Quarterly**, Spring 1997, v. 20, no. 2, p. 80-84. [this is a response to the Vlahos article]

McAuliffe, Daniel J. “Command, Control, Communications, and Intelligence.” **Aerospace America**, December 1994, v. 32, no. 12, p. 35-36.

McConnell, J. M. and Edward J. Giorgio. “Building Information Security Layer by Layer.” **United States Naval Institute Proceedings**, December 1998, v. 124, no. 12, p. 44-47.

McCrohan, Kevin F. “Competitive Intelligence: Preparing for the Information War.” **Long Range Planning**, August 1998, v. 31, no. 4 p. 586-593.

McCutcheon, Chuck. “Pentagon’s Simulated Attacks on Computers Succeed Too Well.” **CQ Weekly**, June 13, 1998, v. 56, no. 24, p. 1622-1623.

McGinnis, Michael L. and George F. Stone. “Decision Support Technology.” **Military Review**, November 1994, v. 74, no. 12, p. 68-75.

McHale, John. “Information Warfare Highlights One of the Most Distressing Weaknesses of COTS.” **Military & Aerospace Electronics**, October 1999, v. 10, no. 10, p. 14-16.

McKenna, James T. "Rome Lab Targets Info Warfare Defenses." **Aviation Week & Space Technology**, August 12, 1996, v. 145, no. 7, p. 65+

McKenna, Pat. “Hacker Trackers: OSI (Office of Special Investigations) Computer Cops Fight Crime On-line.” **Airman,** April 1996, v. 40, no. 4, p. 24-29.

_____. “Info Warriors.” **Airman**, September 1996, v. 40, no. 9, p. 26-31.

_____. “What's the Big Idea? (Information Warfare Battlelab).” **Airman**, October 1998, v. 42, no. 10, p. 34-35.

McLamb, Joseph S. "Future of Mission Orders." **Military Review**, September-October 1997, v. 77, no. 5, p. 71-74.

Meadows, Sandra I. “Information Warriors Raze Enemy's Vital Data Chains.” **National Defense**, March 1995, v. 79, no. 506, p. 30-31.

Meigs, Montgomery C. "Challenges for Army Leaders in an Age of Rapid Change." **Field Artillery,** May-June 1998, p. 3-6.
http://sill-www.army.mil/FAMAG/1998/MAY_JUN_1998/MAY_JUN_1998_FULL_EDITION.pdf

Menoher, Paul E. “Where Do We Go From Here?” **American Intelligence Journal**, Spring-Summer 1994, v. 15, no. 1, p. 11+

Messmer, Ellen. “Facts Fight Fiction in Security Circles.” **Network World**, March 9, 1998, v. 15, no. 10, p. 1+

_____. “Feds Fine-Tune Infowar Plan.” **Network World**, September 14, 1998, v. 15, no. 37, p. 8+

_____. “Feds Plan for Hack Attacks.” **Network World**, October 20, 1997, v. 14, no. 42, p. 43.

Metz, Steven. “Racing Toward the Future: the Revolution in Military Affairs.” **Current History**, April 1997, v. 96, no. 609, p. 184-188.

Metzgar, Terry. "Hostile Intercepts Aimed at Information Systems." **National Defense**, May-June 1993, v. 77, no. 488, p. 24-26.

“Military Operations Must Vie for, Capture Bandwidth.” **Signal**, November 1996, v. 51, no. 3, p. 41-45.

Miller, Ralph and Bryan R. Leipper. “Regarding War.” **Communications of the ACM**, July 1997, v. 40, no. 7, p. 23-24.

Minihan, Kenneth A. “Conflict in the Information Age: Threat and Response.” **American Intelligence Journal**, Spring-Summer 1996, v. 17, no. 1-2, p. 7-10.

_____. “Intelligence and Information Systems Security: Partners in Defensive Information Warfare.” **Defense Intelligence Journal**, Spring 1996, v. 5, no.1, p. 13-23.

“Modern Battlefields Demand Stalwart Industry Practices.” **Signal**, April 1996, v. 50, no. 8, p. 43-46.

Modestov, Sergei A. “The Possibilities for Mutual Deterrence: A Russian View.” **Parameters**, Winter 1996/1997, v. 26, no. 4, p. 92-98.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." **Parameters**, Autumn 1996, v. 26, no. 3, p. 81-92. *http://carlisle-www.army.mil/usawc/Parameters/96autumn/moLander.htm*

Moore, C., et al. "Intelligent Agent-Based Information Warfare Advisor ('Bob-in-a-Box')." **Kybernetes**, 1998, v. 27, no. 1, p. 38+

Morris, Chris, et al. "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos." **Airpower Journal**, Spring 1995, v. 9, no. 1, p. 15-29.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/morris.htm

Morrison, David C. "Bang! Bang! You've Been Inhibited." **National Journal**, March 28, 1992, v. 24, no. 13, p. 758-759.

Morrocco, John D. "Gripen Upgrades Boost Info Warfare Focus." **Aviation Week & Space Technology**, August 3, 1998, v. 149, no. 5, p. 59-61.

_____. "U.K. Launches Review of Defense Priorities." **Aviation Week & Space Technology**, June 2, 1997, v. 146, no. 23, p. 27+

Morton, Oliver. "The Ties That Bind." **The Economist**, June 10, 1995, v. 335, no. 7918, p. SS18+

Mowery, Beverly P. "Technology Opens New Strategies for Future Battlefield Operations." **Signal**, August 1994, v. 48, no. 12, p. 61.

"Multilevel Security Ensures Hardy Information Integrity." **Signal**, June 1997, v. 51, no. 10, p. 93-94+

Munro, Neil. "Inducting Information." **National Journal**, March 27, 1999, v. 31, no. 13, p. 818-824.

_____. "Information Warfare Policies Emerge." **Washington Technology**, July 27, 1995, v. 10, no. 8, p. 1.

_____. "Infowar: AK-47s, Lies, and Videotape." **Communications of the ACM**, July 1999, v. 42, no. 7, p. 19-22.

_____. "Infowar Disputes Stall Defense Policy." **Washington Technology**, May 25, 1995, v. 10, no. 4, p. 1.

_____. "Sketching a National Information Warfare Defense Plan." **Communications of the ACM**, November 1996, v. 39, no. 11, p. 15-17.

_____. “U.S. Boosts Information Warfare Initiative.” **Defense News**, January 25-31, 1993, v. 8, p. 1+

Munro, Neil and Barbara Opall. “Military Studies Unusual Arsenal.” **Defense News**, October 19-25, 1992, v. 7, p. 3+

Muradian, Vago. “F-22 Would Accommodate ‘Information Warfare’ Applications.” **Defense Daily**, December 10, 1996, v. 193, no. 47, p. 1.

Mussington, David. "Throwing the Switch in Cyberspace (Emergence of Global Information Networks)." **Jane's Intelligence Review**, July 1996, v. 8, no. 7, p. 331-334.

Naylor, Sean D. “Info War: ‘Digitization’ Will Shape How Future Wars are Fought.” **Army Times**, May 17, 1993, v. 53, p. 12-14.

Neilson, Robert E. and Daniel T. Kuehl. “Evolutionary Change in Revolutionary Times: a Case for a New National Security Education Program.” **National Security Studies Quarterly**, Autumn 1999, v. 5, no. 4, p. 29-41

Nekoba, Barbara. "Open Source Information and the Marine Corps." **Marine Corps Gazette**, June 1997, v. 81, no. 6, p. 38-40.

Newland, Ronald K. “Tactical Deception in Information Warfare: A New Paradigm for C4I.” **Journal of Electronic Defense**, December 1998, v. 21, no. 12, p. 43-50.

Nicholls, David and Todar D. Tagarev. “What Does Chaos Theory Mean to Warfare?” **Airpower Journal**, Fall 1994, v. 8, no. 3, p. 48-57.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj94/fal94/nichols.html

Nowowiejski, Dean A. "Achieving Digital Destruction: Challenges for the M1A2 Task Force." **Armor**, January-February 1995, v. 104, no. 1, p. 21-24.

Nye, Joseph S., Jr. and William A. Owens. “America’s Information Edge.” **Foreign Affairs**, March-April 1996, v. 75, no. 2, p. 20-36.

O’Malley, Chris. “Information Warriors of the 609th.” **Popular Science**, July 1997, v. 251, no. 1, p. 70-74.

Owens, William A. “The American Revolution in Military Affairs.” **Joint Force Quarterly**, Winter 1995/1996, no. 10, p. 37-38.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1010.pdf

_____. "Emerging System of Systems." **United States Naval Institute Proceedings**, May 1995, v. 121, no. 5, p. 35-39.

Paige, Emmett, Jr. “Achieving the Integrated Systems Concept.” **Defense Issues**, 1996, v. 11, no. 51, p. 1-4.
http://www.defenselink.mil/speeches/speech.aspx?speechid=1015

_____. “Ensuring Joint Force Superiority in the Information Age.” **Defense Issues**, July 30, 1996, v. 11, no. 82, p. 1-4.
http://www.defenselink.mil/speeches/speech.aspx?speechid=961

Panda, Brajendra and Joseph Giordano. “Defensive Information Warfare.” **Communications of the ACM**, July 1999, v. 42, no. 7, p. 30-32.

Pathak, A.K., Zafar Husain, and R. D. Pathak. “Technology-Based Information Warfare: Developing World Perspective.” **International Journal of Computer Applications in Technology**, 2003, v. 16, no. 1, p. 47-53.

Peniston, Bradley. “Info Warriors: The Hot New Career Paths.” **Navy Times**, July 26, 1999, v. 48, no. 42, p. 14-15.

“Pentagon Found Ill-Prepared for Asymmetric Warfare.” **Defense Daily**, October 8, 1997, v. 197, no. 6, p. 1+

Peters, Ralph. "Constant Conflict." **Parameters**, Summer 1997, v. 27, no. 2, p. 4-14.

_____. “New Strategic Trinity.” **Parameters**, Winter 1998, v. 28, no. 4, p. 73-79.
http://carlisle-www.army.mil/usawc/Parameters/98winter/peters.htm

Petersen, John L. “Info War: The Next Generation.” **United States Naval Institute Proceedings**, January 1997, v. 123, no. 1, p. 60-62.

Petersen, John H. “Info Wars.” **United States Naval Institute Proceedings**, May 1993, v. 119, no. 3, p. 85-92.

Peterson, Padgett. “Tactical Computers Vulnerable to Malicious Software Attacks.” **Signal**, November 1993, v. 48, no. 3, p. 74-75.

"Planners Seek New Models to Study Information Wars." **National Defense**, July-August 1996, v. 81, no. 519, p. 57.

Platt, Charles. “Hackers: Threat or Menace?” **Wired**, November 1994, v. 2, no. 11, p. 82+
http://www.wired.com/wired/archive/2.11/hack.cong.html

Ploskina, Brian. “Government Warns of Information Warfare.” **ENT**, August 12, 1998, v. 3, no. 13, p. 3.

“Plug-and-Play Naval Network Profits from New Technology: Navy's Copernicus Vision for Command, Control, Information Warfare Focuses on Joint Systems.“ **National Defense**, December 1996, v. 81, no. 523, p. 30-31.

"Policy Forum: Pearl Harbor in Information Warfare?" **The Washington Quarterly**, Spring 1997, v. 20, no. 2, p. 39+

Porter, Tim. “Information Warfare - Your Company Needs You!” **Computers & Security**, 1996, v. 15, no. 5, p. 414.

_____. “Information Warfare - Your Company Needs You!” **Computers & Security**, 1996, v. 15, no. 7, p. 561-566.

Potter, David L. “Information Warfare: Malicious Software and Technology.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 34-37.

Powell, Colin L. “Information-Age Warriors.” **Byte**, July 1992, v. 17, no. 7, p. 370.

Power, Richard. “CSI Special Report on Information Warfare.” **Computer Security Journal**, Fall 1995, v. 11, no. 2, p. 63+

Pozdnyakov, Aleksandr, Interviewed by Vladimir Davydov, "Information Security," Granitsa Rossii, September 1995, p. 6-7, trans. in FBIS-UMA-95-239-S, 13 December 1995, p. 41-44.

Prina, L. Edgar. "Forum for the Future: Record Crowd at CSF (Current Strategy Forum) '95." **Sea Power**, August 1995, v. 38, no. 8, p. 37-39.

Ragsdale, D.J., Scott D. Lathrop and Ronald C. Dodge. “Enhancing Information Warfare Education Through the Use of Virtual and Isolated Networks.” **Journal of Information Warfare**, 2003, v. 2, no. 3, p. 47-59.

Rannou, Jean. “Information in the Use of Air Power.” **Military Technology**, May 1999, v. 23, no. 5, p. S12-S14.

"Rapid Technology Growth Spawns Land Information Warfare Activity." **Signal**, July 1996, v. 50, no. 11, p. 51-54.

Rathmell, Andrew. “INFORMATION WARFARE - USA tackles Cyber Threat.” **Jane's Intelligence Review**, September 1, 1998, [Pointer Edition], p.14.

Rawnsley, Gary D. “Old Wine in New Bottles: China-Taiwan Computer-Based ‘Information Warfare’ and Propaganda.” **International Affairs**, October 2005, v. 81, no. 5, p. 1061-1078

Reardon, Thomas M. “Information Warfare: Protecting Force Sustainment.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 25-27.

“Redundancy, Robustness Protect Vital National Information Links.” **Signal**, May 1996, v. 50, no. 9, p. 36-39.

Reitlinger, Kurt C. “Command and Control for Third Wave Warfare.” **Army**, February 1995, v. 45, no. 2, p. 9.

Remenyi, D. “e-Democracy – An Invitation to I-Warfare?” **Journal of Information Warfare**, March 2003, v. 2, no. 2.

Rhea, John. “COTS Eyed for Information Warfare.” **Military & Aerospace Electronics**, September 1997, v. 8, no. 9, p. 12-14.

_____. “The Dilemma of Using COTS in Electronic Warfare Systems” **Military & Aerospace Electronics**, September 1996, v. 7, no. 9, p. 8-10.

Rhode, William E. “What is Info Warfare.” **United States Naval Institute Proceedings**, February 1996, v. 122, no. 2, p. 34-41.

Rhodes, Christopher J. “Information Warfare: How Real is the Threat and Can it be Countered?” **Military Technology**, 2001, v. 25, no. 5, p. 71-73.

Riccardelli, Richard F. "Information and Intelligence Revolution." **Military Review**, September-October 1995, v. 75, no. 5, p. 82-87.

Richardson, Doug. "Hacker Warfare: Threat of the Future?" **Armada International**, August-September 1997, v. 21, no. 4, p. 64-66+

_____. "Information Warfare--New Threats and New Opportunities." **Asian Defence Journal**, April 1997, no. 4, p. 50-55.

“Risk Management Provides Vital Information Security.” **Signal**, October 1994, v. 49, no. 2, p. 25-28.

Rivera, Rose. “LIWA [Land Information Warfare Activity].” **INSCOM Journal**, May-June 1997, v 20, no. 3, p. 20-21.

Robinson, Clarence A., Jr. “Bolstering Data Defenses.” **Signal**, July 1998, v. 52, no. 11, p. 23+

_____. “Bosnia’s Information River Slows, Trickles to Soldiers.” **Signal**, June 1997, v. 51, no. 10, p. 87-90.

_____. “China’s Military Potency Relies on Arms Information Content.” **Signal**, November 1999, v. 54, no. 3, p. 21-28.

_____. “Commanders Pull Intelligence in Information Warfare Strategy.” **Signal**, August 1994, v. 48, no. 12, p. 29-31.

_____. "Defense Organization Safeguards War Fighters' Information Flow." **Signal**, October 1995, v. 50, no. 2, p. 15-18.

_____. “Electronic Battlefield’s Exposure Bolsters Army.” **Signal**, August 1991, v. 45, no. 12, p. 18-24.

_____. “Electronic Combat Techniques Provide Information Edge.” **Signal**, July 1995, v. 49, no. 11, p. 33-35.

_____. “Encryption Issues Dominates Information Warfare Defense.” **Signal**, May 1996, v. 50, no. 9, p. 34.

_____. “Firewall Consortium Expands Cyberspace Security Sagacity.” **Signal**, March 1996, v. 50, no. 7, p. 17-20.

_____. “Information Warfare Demands Battlespace Visualization Grasp.” **Signal**, February 1997, v. 51, no. 6, p. 17-20.

_____. “Information Warfare Strings Trip Wire Warning Strategy.” **Signal**, May 1996, v. 50, no. 9, p. 29-33.

_____. “Intelligence Agency Adjusts as Mission Possible Unfolds.” **Signal**, October 1998, v. 53, no. 2, p. 17-19.

_____. “Redundancy, Robustness Protect Vital National Information Links: Increased Awareness of Risks is Initial Step in Detecting, Reacting to Information Warfare.” **Signal**, May 1996, v. 50, no. 9, p. 36-39.

_____. “Research Objectives Support Joint War Fighter Operations.” **Signal**, January 1997, v. 51, no.5, p. 19-24.

Rodgers, James L. "Information Warfare: Nothing New Under the Sun." **Marine Corps Gazette**, April 1997, v. 81, no. 4, p. 23-29.

Rodionoy, M. A. “Forms of Information Warfare.” **Military Thought**, 1998, v. 7, p. 84-88.

Rohde, William E. “What is Info Warfare?” **United States Naval Institute Proceedings**, February 1996, v. 122, no. 2, p. 34-38.

Romanych, Marc J. “Visualizing the Information Environment.” **Military Intelligence Professional Bulletin**, July-September 2003, v. 29, no. 3, p. 5-8. *http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=265&issueID=19*

Rona, Thomas P. “Information Warfare: An Age Old Concept With New Insights.” **Defense Intelligence Journal**, Spring 1996, v. 5, no.1, p. 53-67.

Ronfeldt, David F. “Cyberocracy is Coming.” **The Information Society**, 1992, v. 8, no. 4, p. 243+

Roos, John G. “Info Tech, Info Power.” **Armed Forces Journal International**, June 1994, v. 131, p. 31-36.

Ropelewski, Robert. “Command, Control Priorities Shift, Steady Funding Persists.” **Signal**, May 1996, v. 50, no. 9, p. 41-44.

Ross, Jimmy D. "Winning the Information War." **Army**, February 1994, v. 44, no. 2, p. 26-28+

Rothrock, John. “Information Warfare: Time for Some Constructive Skepticism.” **American Intelligence Journal**, Spring-Summer 1994, v. 15, no. 1, p. 71-76.

Russo, Anthony J. “Leadership in the Information Age.” **Military Review**, May-June 1999, v. 79, no. 3, p. 77-81.

Ryan, Donald E., Jr. "Implications of Information-Based Warfare." **Joint Force Quarterly**, Autumn-Winter 1994-1995, no. 6, p. 114-116. *http://www.dtic.mil/doctrine/jel/jfq_pubs/impl6.pdf*

Ryan, Julie, John Woloschek and Barry Leven. “Complexities in Conducting Information Warfare.” **Defense Intelligence Journal**, Spring 1996, v. 5, no.1, p. 69-82.

Saint, Crosbie E. and Ronald L. Watts. "Comanche Era Fleet: A Combat Multiplier." **Military Review**, May-June 1995, v. 75, no. 3, p. 39-47.

Sanz, Timothy L. “Information-Age Warfare: A Working Bibliography.” **Military Review**, Pt. 1, v. 78, no. 2 (March-April 1998), p. 83-90; Pt. 2, September-November 1998, v. 78, no. 5, p. 41-50.

Sapolsky, Harvey M., et al. “Security Lessons From the Cold War.” **Foreign Affairs**, July-August 1999, v. 78, no. 4, p. 77-89.

Scales, Robert H., Jr. “Adaptive Enemies: Dealing with the Strategic Threat After 2010.” **Strategic Review**, Winter 1999, v. 27, no. 1, p. 5-14.

_____. "Cycles of War: Speed of Maneuver Will be the Essential Ingredient of an Information-Age Army." **Armed Forces Journal International**, July 1997, v. 134, no. 12, p. 38+

Schiltz, Eugene. “Information Warfare Between China and the US.” **Computers & Security**, 2002, v. 21, no. 4, p. 299-200.

Schneider, James J. "Black Lights: Chaos, Complexity, and the Promise of Information Warfare." **Joint Force Quarterly**, Spring 1997, no. 15, p. 21-28. *http://www.dtic.mil/doctrine/jel/jfq_pubs/07_15.pdf*

Schroer, Ron. “’System Readiness’ Test Technology for the 21st Century.” **IEEE Aerospace and Electronic Systems Magazine**, March 1996, v. 11, no. 3, p. 7-11.

Schwartau, Winn. “’Defense in Depth’ for Information Systems Survival.” **International Journal of Intelligence and Counterintelligence**, Summer 1995, v. 8, no. 2, p. 229-234.

_____. “What Exactly Is Information Warfare?” **Network Security**, Pt. 1, September 1997, v. 1997, no. 9, p. 17-19; Pt. 2, October 1997, v. 1997, no. 10, p. 12-16; Pt. 3, November 1997, v. 1997, no. 11, p. 12-18.

Scott, William B. “Computer/IW Efforts Could Short Change Aircraft Programs.” **Aviation Week & Space Technology**, January 19, 1998, v. 148, no. 3, p. 59.

_____. “'Info Warriors' Given New Clout.” **Aviation Week & Space Technology**, February 1, 1999, v. 150, no. 5, p. 64-65.

_____. "'Information Warfare' Demands New Approach." **Aviation Week & Space Technology**, March 13, 1995, v. 142, no. 11, p. 85+

_____. "Information Warfare Policies Called Critical to National Security." **Aviation Week & Space Technology**, October 28, 1996, v. 145, no. 18, p. 60+

Seagraves, Mary Ann and Richard J. Szymber. “Owning the Weather: the Environmental Side of the Information War.” **Army RD&A Bulletin**, March 1995, no, 2, p. 30-32.

"Security Safeguards Primary Battlefield Support Criterion." **Signal**, November 1996, v. 51, no. 3, p. 40.

Seffers, George I. “Hackers are Using New and Old Techniques.” **Air Force Times**, November 16, 1998, v. 59, no. 15, p. 14.

_____. “Hackers Complain Pentagon’s Not Playing Fair.” **Air Force Times**, October 12, 1998, v. 59, no. 10, p. 36.

_____. “Inventor Spawns 'Electronic Ebola' for Info War.” **Defense News**, June 15-21, 1998, v. 13, p. 1+

_____. “’Joint Doctrine’ Spurs Information Arms Race.” **Army Times**, November 23, 1998, v. 59, no. 17, p. 26.

_____. “Pentagon Resurrects Top C3I Office: Overturns Closure Decision, Adds Space, Infotech Roles.” **Defense News**, February 16-22, 1998, v. 13, p. 1+

_____. “Thwarted Hackers Call Pentagon Actions ‘Offensive.’” **Army Times**, October 12, 1998, v. 59, no. 11, p. 31.

_____. ”U.S. Congress Attacks Cyber Defense Funds.” **Defense News**, June 15-21, 1998, v. 13, p. 3+

Seigle, Greg. “New Information Warfare Strategy.” **Jane’s Defence Weekly**, June 30, 1999, v. 31, no. 26, p. 9.

“Select Enemy. Delete.” **Economist**, March 8, 1997. v. 342, no. 8007, p. 21+

Serookiy, Yu Ye. “Psychological-Information Warfare: Lessons of Afghanistan.” **Military Thought**, 2004, v. 13, no. 1, p. 196-200.

Shalikashvili, John M. "Building Foundation of America's Forces for 21st Century." **The Officer**, February 1997, v. 73, no. 2, p. 28-34.

Sharma, Sushil K. and Jatinder N. Gupta. “Securing Information Infrastructure from Information Warfare.” **Logistics Information Management**, 2002, v. 15, no. 5/6, 414-422.

Shelton, H. Hugh. “Winning the Information Warfare in Haiti.” **Military Review**, November-December 1995, v. 75, no. 6, p. 3-9.

Shelton, Paul A. “Frontline Intelligence for the 21st Century.” **Marine Corps Gazette**, September 1996, v. 80, no. 9, p. 30-39.

Sherman, Jason. "Infowar: What Kind of a Defense?" **Armed Forces Journal International**, August 1997, v. 135, no. 1, p. 28+

_____. “Welcome to the Future: The US Army Tests Its Information-Age Brigade in the Desert.” **Armed Forces Journal International**, May 1997, v. 134, no. 10, p. 12-13.

“Signals Intelligence & Information War.” **American Intelligence Journal**, Spring/Summer 1994, v. 15, no. 1. Entire Issue.

Singer, Abe and Scott Rowell. "Information Warfare: An Old Operational Concept With New Implications." **Strategic Forum**, December 1996, no. 99. 4p. *http://www.ndu.edu/inss/strforum/SF_99/forum99.html*

Singh, Ajay. “The Fundamentals of Information Warfare.” **Strategic Analysis**, November 1995, v. 18, no. 8, p. 1047+

_____. “Time: The New Dimension in War.” **Joint Force Quarterly**, Winter 1995/1996, no. 10, p. 56-61. *http://www.dtic.mil/doctrine/jel/jfq_pubs/1510.pdf*

Sizer, Richard A. “Land Information Warfare Activity: IO and IW Support to Army XXI.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 23-24.

Smith, Bruce T. “An Eye for an Eye, a Byte for a Byte.” **Federal Lawyer**, October 1995, v. 42, no. 9, p. 12-13.

Smith, Edward A., Jr. "Putting it Through the Right Window." **United States Naval Institute Proceedings**, June 1995, v. 121, no. 6, p. 38-40.

Smith, Irene M. “Information Warfare.” **Surface Warfare**, March/April 1999, v. 24, no. 2, p. 20-23.

Smith, George. “An Electronic Pearl Harbor? Not likely.” **Issues in Science and Technology**, Fall 1998, v. 15, no. 1, p. 68-73.

Smith, William D. “Information Warfare, It's Here to Stay!” **Naval Forces**, 2000, v. 21, no. 1, p. 35-37.

Smolyan, Georgiy, Vitaliy Tsygichko, and Dmitriy Chereshkin, "A Weapon That May Be More Dangerous Than a Nuclear Weapon: The Realities of Information Warfare," **Nezavisimoye Voyennoye Obozreniye**, 18 November 1995, Supplement No. 3, p. 1-2, trans. in FBIS-UMA-95-234-S, 6 December 1995, p. 31-35.

Smullen, Robert J. “Infantryman's RMA (Revolution in Military Affairs).” **Marine Corps Gazette**, January 1996, v. 80, no. 1, p. 22-23.

Souder, Jeffery and Richard McCrary. “Signal Center Uses Advanced Modeling Tools to Design Warfighter Information Network.” **Army Communicator**, Summer 1998, v. 23, no. 3, p. 36-38.

Spiszer, John M. "FM (Field Manual) 100-5 and Information Age Warfare." **Military Review**, September-October 1997, v. 77, no. 5, p. 15-18.

Stanton, John. "Dilemmas Abound in Crafting National Information Policy." **National Defense**, July-August 1997, v. 82, no. 529, p 52-54.

_____. “White House Plans Cyber Homeland Defense Effort.” **National Defense**, September 1998, v. 83, no. 540, p. 24-25.

Starr, Barbara. "US `Puzzle Palace' (National Security Agency) Seeks New Clues to Combat Old Threats." **Jane’s Defence Weekly**, September 3, 1997, v. 28, no. 9, p. 35-36.

Stauffer, Don. “Electronic Warfare: Battles Without Bloodshed.” **Futurist**, January/February 2000, v. 34, no. 1, p. 23-26.

Stavridis, James. “The Second Revolution.” **Joint Force Quarterly**, Spring 1997, no. 15, p. 8-13. *http://www.dtic.mil/doctrine/jel/jfq_pubs/05_15.pdf*

Steele, Robert D. “The Asymmetric Threat: Listening to the Debate.” **Joint Force Quarterly**, Autumn/Winter 1998-1999, no. 20, p. 78-84. *http://www.dtic.mil/doctrine/jel/jfq_pubs/1520.pdf*

_____. "Smart Nations: Achieving National Security and National Competitiveness in the Age of Information." **Bulletin of the American Society for Information Science**, October/November 1996, v. 23, no. 1, p. 8-10

Stein, George J. "Information Warfare." **Airpower Journal**, Spring 1995. v. 9, no. 1, p. 30-39. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/stein.htm*

Stephens, Alan. “The Knowledge Edge.” **Asia-Pacific Defence Reporter**, April-May 1999, v. 25, no. 3, p. 56-57.

Stephenson, Peter. “Information Warfare, or, Help! The Sky is Falling.” **Information Systems Security**, Spring 1999, v. 8, no. 1, p. 6-10.

Sterner, Eric R. “Digital Pearl Harbor: National Security in Information Age.” **National Security Studies Quarterly**, Summer 1996, v. 2, no. 3, p. 33-35.

Stewart, John F. "Intelligence Strategy for the 21st Century." **Military Review**, September-October 1995, v. 75, no. 5, p. 75-81.

Stix, Gary. “Fighting Future Wars.” **Scientific American**, December 1995, v. 273, no. 6, p. 92-98.

“Strategic Information Warfare.” **The Futurist**, September/October 1997, v. 31, no. 5, p. 15.

Strickland, Frank B., Jr. "It's Not About Mousetraps--Measuring the Value of Knowledge for Operators." **Joint Force Quarterly**, Autumn 1996, no. 13, p. 90-96. *http://www.dtic.mil/doctrine/jel/jfq_pubs/1913.pdf*

Struble, Dan. "What is Command and Control Warfare?" **Naval War College Review**, Summer 1995, v. 48, no. 3, p. 89-98.

Studemeister, Margarita S. “The Impact of Information and Communication Technologies on International Conflict Management.” **Bulletin of the American Society for Information Science**, February/March 1998, v. 24, no. 3, p. 24-27.

Sullivan, Gordon R. “A New Force for a New Century.” **Army**, May 1994, v. 44, no. 5, p. 24+

Sullivan Gordon R. and James M. Dubik. “War in the Information Age.” **Military Review**, April 1994, v. 74, no. 4, p.46-62.

Swan, Patrick A. “The Ethics of Photo Digital Manipulation.” **Military Review**, November/December 1995, v. 75, no. 6, p. 80-81.

Sweetnam, J.P. "New Thinking in the US Army: The Louisiana Manoeuvres, Battle Laboratories and the Third Wave Army." **Canadian Defence Quarterly**, September 1994, v. 24, no. 1, p. 23-28.

Swett, Charles. "Review Essay: War and Anti-War." **Special Warfare**, January 1995, v. 8, no. 1, p. 26-31.

“System Detects Cyber Break-Ins.” **Signal**, November 1997, v. 52, no. 3, p. 6.

Szafranski, Richard. “Neocortical Warfare? The Acme of Skill.” **Military Review**, November 1994, v. 74, no. 12, p. 41-55.

_____. “Parallel War: Promise and Problems.” **United States Naval Institute Proceedings**, August 1995, v. 121, no. 8, p. 57-61.

_____. "A Theory of Information Warfare: Preparing for 2020." **Airpower Journal**, Spring 1995, v. 9, no. 1, p. 56-65.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm

_____. “When Waves Collide: Future Conflict.” **Joint Force Quarterly**, Spring 1995, no. 7, p 77-84.
http://www.dtic.mil/doctrine/jel/jfq_pubs/jfq1807.pdf

Szewczak, Edward. “Information Warfare and Security.” **Information Resources Management Journal**, April-June 1999, v. 12, no. 2, p. 38.

Szymber, Richard J. “Owning the Weather: Weather Support to Force XXI.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 42-45, 48.

Tapscott, Mark and Kay Atwal. “New Weapons that Win Without Killing on DoD’s Horizon.” **Defense Electronics**, February 1993, v. 25, no. 2, p. 41-46.

Taylor, John W. “Strategic Military Employment Options: Theory and Applications.” **Comparative Strategy**, April/June 1991, v. 10, no. 2, p. 155-164.

Tempestilli, Mark. “Network Force (Information Warfare).” **United States Naval Institute Proceedings**, June 1996, v. 122, no. 6, p. 42-46.

Thayer, Bradley A. “The Political Effects of Information Warfare: Why New Military Capabilities.” **Security Studies**, Autumn 2000, v. 10, no. 1, p. 43-85.

Thomas, Tim. “Confrontation Central to Chinese IW (Information Warfare) Aims.” **Jane’s Intelligence Review**, June 2002, v. 14, no. 6, p. 52-53.

Thomas, Timothy L. "Age of the New Persuaders." **Military Review**, May-June 1997, v. 77, no. 3, p. 72-80.

_____. "Deterring Information Warfare: A New Strategic Challenge." **Parameters**, Winter 1996-1997, v. 26, no. 4, p. 81-91.
http://carlisle-www.army.mil/usawc/Parameters/96winter/thomas.htm *OR*
http://fmso.leavenworth.army.mil/documents/deteriw.htm

_____. “Human Network Attacks.” **Military Review**, September/October 1999, v. 79, no. 5, p. 23-33.

_____. “Infosphere Threats.” **Military Review**, September/October 1999, v. 79, no. 5, p. 46-51.
http://fmso.leavenworth.army.mil/documents/infosphere/infosphere.htm

_____. “The Internet in China: Civilian and Military Uses**.” Information & Security, An International Journal**, 2001, v. 7, p. 159-173
*http://fmso.leavenworth.army.mil/documents/china-internet.*htm

_____. “Is the IW Paradigm Outdated? A Discussion of U.S. I.W. Theory.” **Journal of Information Warfare**, 2003, v. 2, no. 3, p. 109-116.
http://fmso.leavenworth.army.mil/documents/InfoWar.pdf

_____. “Like Adding Wings to a Tiger – Chinese Information War Theory and Practice.” **Military Intelligence Professional Bulletin**, July-September 2003, v. 29, no. 3, p. 22-27.
http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=270&issueID=19

_____. "The Mind Has No Firewall." **Parameters**, Spring 1998, v. 28, no. 1, p. 84-92. *http://carlisle-www.army.mil/usawc/Parameters/98spring/thomas.htm*

_____. “Russia's Information Warfare Structure: Understanding the Roles of the Security Council, FAPSI (Federal Agency for Government Communications and Information), the State Technical Commission and the Military.” **European Security**, Spring 1998, v. 7, no. 1, p. 156-172.

_____. “Russian Views on Information-Based Warfare.” **Airpower Journal**, 1996, v. 10, Special Edition, p. 25-35. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/spec96/thomas.html* OR *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/spec96/thomas.pdf*

Tirpak, John A. "The New World of Information Warfare." **Air Force Magazine**, June 1996, v. 79, no. 6. p. 30-35.

Todd, David. “Gird for Information War: U.S. Must Control Combat in Cyberspace Front.” **Defense News**, March 6, 1995, v. 10, p. 20+

Toffler, Alvin. “Knowledge-Based Strategies Propel Software Over Steel.” **Signal**, April 1994, v. 48, no. 4, p. 49+

Tomes, Robert R. “Boon or Threat? The Information Revolution and U.S. National Security.” **Naval War College Review**, Summer 2000, v. 53, no. 3, p. 39-59.

Triplett, William C., II. “Potential Applications for PLA Information Warfare Capabilities to Critical Infrastructures.” **Hampton Roads International Security Quarterly**, June 2002, p. 185-212.

Turner, Jackie. “Emergence and Convergence: Information Warfare in the Early 20th Century.” **Spokesman**, October 1994, v. 34, no. 9, p. 17-18.

Ullman, Harlan K. "New Defence Construct: ‘Rapid Dominance.'" **RUSI Journal**, October 1996, v. 141, no. 5, p. 8-12.

“U.S. Seeks Alliance Support for Infrastructure Protection.” **Signal**, July 1998, v. 52, no. 11, p. 29-32.

Valeri, Lorenzo. "Guarding Against a New Digital Enemy." **Jane's Intelligence Review**, August 1997, v. 9, no. 8, p. 379-382.

Valli, Craig. “Personalised Information Warfare – The New Homeland Defense.” **Journal of Information Warfare**, October 2002, v. 2, no. 1.

Valovic, Tom. “Information Warfare Hits the Telecom Industry...and It's Not a Pretty Picture.” **Telecommunications** [Americas ed.], October 1996, v. 30, no. 10, p. 8.

Vanderbilt, T. “Global Hacking.” **Rolling Stone**, November 11, 1999, no. 825, p. 39-40.

Venzke, Ben. “Information Warrior.” [Interview With Winn Schwartau]. **Wired**, August 1996, v. 4, no. 8, p. 136-137.
http://www.wired.com/wired/archive/4.08/schwartau.html

Verton, Daniel. “DOD Faces Infowar Controls.” **Federal Computer Week**, January 11, 1998, v. 13, no. 1, p. 10-11.

Vincent, Gary A. “A New Approach to Command and Control: The Cybernetic Design.” **Airpower Journal**, Summer 1993, v. 7, no. 2, p. 24-38.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj93/sum93/vincent.htm

Vistica, Gregory L. and Evan Thomas. “The Secret Hacker Wars.” **Newsweek**, June 1, 1998, v. 131, no. 22, p. 60-61.

Vlahos, Michael. “The War After Byte City.” **Washington Quarterly**, Spring 1997, v. 20, no. 2, p. 41-72.

Wall, Robert. “USAF Expands Infowar Arsenal.” **Aviation Week & Space Technology**, November 15, 1999, v. 151, no. 20, p. 102+

Wallace, Eric S. “Athena: A Structured and Logical Approach to Information Operations Planning.” **Cyber Sword**, Fall 1997, v. 1, no. 2, p. 27-29.

Walls, A. “The Image of Unanimity: The Utility of the Promotion and Disparagement of Cultural and Social Unanimity as a Form of Context Manipulation in Information Warfare in the Aftermath of the Attacks of September 11, 2001.” **Journal of Information Warfare**, March 2003, v. 2, no. 2.

Walsh, Edward J. "Pentagon Joins Other Federal Agencies in New Managed Information Strategy." **National Defense**, July-August 1997, v. 82, no. 529, p. 50-51.

Walsh, Mark. “U.S. Military Expands Information Warfare Defenses.” **Defense News**, April 28-May 4, 1997, v. 12, p. 25.

Walsh, Robert S. "Information Enhancement on Today's Battlefield." **Marine Corps Gazette**, October 1995, v. 79, no. 10, p. 27-29.

Waltz, Edward. “US Transition to Information Warfare.” **Journal of Electronic Defense**, December 1998, v. 21, no. 12, p. 35-42.

Wang, Vincent Wei-cheng and Gwendolyn Stamper. “Asymmetric War? Implications for China’s Information Warfare Strategies.” **American Asia Review**, Winter 2002, v. 20, no. 4, p. 167-207.

Warden, John A. “The Enemy as a System.” **Airpower Journal**, Spring 1995, v. 9, no. 1, p. 40-55.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm

Wardynski, E. Casey. "Labor Economics of Information Warfare." **Military Review**, May-June 1995, v. 75, no. 3, p. 56-61.

Webb, R. C., et al. “The Commercial and Military Satellite Survivability Crisis.” **Defense Electronics**, August 1995, v. 27, no. 8, p. 21+

Weible, Jack. "Vulnerable to Attack? Subcommittees Get an Earful on Threats to Information Systems." **Air Force Times**, April 14, 1997, v. 57, no. 37, p. 28.

Welch, Jonathan. “International Money Market: A Weapon in Waiting?” **RUSI Journal**, April 1996, v. 141, no. 2, p. 34-40.

Wheeler, Douglas L. “Spy Mania and the Information War: The Hour of the Counterspy, 1914/1915.” **American Intelligence Journal**, Autumn-Winter 1992-1993, v. 14, no. 1, p. 41-45.

Whitehead, YuLin. "Information as a Weapon: Reality Versus Promises." **Airpower Journal**, Fall 1997, v. 11, no. 3, p. 40-54.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj97/fal97/whitehead.htm
OR *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj97/fal97/whitehead.pdf*

Wilkin, Dale. “Command and Control Warfare: Providing the Right Info, to the Right Place, at the Right Time.” **Spokesman**, October 1994, v. 34, no. 9, p. 13-14.

Williams, Cindy. “Information and Command and Control.” **Aerospace America**, December 1998, v. 36, no. 12, p. 48-49.

Williams, Robert H. "Info Warfare Attacks Score in Military's Risk Pantheon." **National Defense**, September 1996, v. 81, no. 520, p. 16-17.

Williamson, John. "Winning the Data War." **Jane’s Defence Weekly**, May 20, 1995, v. 23, no. 20, p. 44-46.

Wilson, G. I. and Frank Bunkers. "Uncorking the Information Genie." **Marine Corps Gazette**, October 1995, v. 79, no. 10, p. 29-31.

Wilson, George C. “Army Tests Information Technology: Defense Secretary Sees a ‘Revolution' in Warfare.” **Air Force Times**, April 7, 1997, v. 57, no. 36, p. 26.

Wilson, Jim. “Information Warfare.” **Popular Mechanics**, March 1999, v. 176, no. 3, p. 58-61.

Wilson Johnnie W. "Information Age Army." **Army**, June 1997, v. 47, no. 6, p. 14-16+

Wilson, William F. “Despite Computer Security Advances, Hackers Appear to be Keeping Pace.” **National Defense**, September 1998, v. 83, no. 540, p. 26.

Wood, C. Norman. “Networks Crucial Key to Information Supremacy.” **Signal**, July 1997, v. 51, no. 11, p. 14.

Wood, John Robert. “Lessons Learned in Information Age Warfare.” **Army**, February 1996, v. 46, no. 2, p. 32+

Wriston, W. B. “Bits, Bytes and Diplomacy.” **Foreign Affairs**, September-October 1997, v. 76, no. 5, p. 172-182.

Wyly, Michael D. “Fourth Generation Warfare: What Does It Mean to Every Marine?” **Marine Corps Gazette**, March 1995, v. 79, no. 3, p. 55-58.

Zimmerman, Stan. "The Battle of the Lasting Impression." **United States Naval Institute Proceedings**, May 1997, v. 123, no. 5, p. 44-47.

Documents, Theses & Technical Reports

Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography.

Adamiec, Raymond. ***Information Warfare: Evaluating Information Targets***. Newport, RI: Naval War College, 14 June 1996. 26p.

Abstract: Information Warfare in its broadest definition has existed since armed conflict began. As the pace of battle accelerates and information collection intensifies it is necessary to have a means of synergistically combining the advanced technological tools, organizational structure and mathematical analysis of information target vulnerabilities. This essay provides a model to accomplish such a goal by establishing a framework to evaluate methods of employment, types of attack and desired results when prioritizing information targets.

ACCESSION NUMBER: ADA312069

http://handle.dtic.mil/100.2/ADA312069

Ammann, P., et al. "Surviving Information Warfare Attacks on Databases." p. 164-174, IN: ***Security and Privacy***, 1997. Proceedings, 1997 IEEE Symposium, 4-7 May 1997. 249p.

Abstract: We consider the problem of surviving information warfare attacks on databases. We adopt a fault tolerance approach to the different phases of an attack. To maintain precise information about the attack, we mark data to reflect the severity of detected damage as well as the degree to which the damaged data has been repaired. In the case of partially repaired data, integrity constraints might be violated, but data is nonetheless available to support mission objectives. We define a notion of consistency suitable for databases in which some information is known to be damaged, and other information is known to be only partially repaired. We present a protocol for normal transactions with respect to the damage markings and show that consistency preserving normal transactions maintain database consistency in the presence of damage. We present an algorithm for taking consistent snapshots of databases under attack. The snapshot algorithm has the virtue of not interfering with countermeasure transactions.

Anderson, Christina M. ***Development of a National Information Warfare Strategy: A Reengineering Approach***. Maxwell AFB, AL: Air University, Center for Aerospace Doctrine, Research, and Education, December 1997. 93p.

Abstract: This thesis presents an analysis of the United States' national strategy for defensive against information warfare (IW). Vast improvements in technology have created new problem areas regarding U.S. national security and strategy. National security is now threatened by potential attacks on our national infrastructure. The need for defense against such attacks continues to grow as a national security problem. However, there is currently no national direction in this increasingly critical area of national security. Regarding this need for a national IW policy, the following questions are investigated: (1) How and by whom is the U.S. ensuring reliability and security of its information. (2) Are current key organizations in IW, and their associated strategies, adequately defending the U.S. against the threat of IW. (3) Is there a need for a national IW strategy to successfully defend against information warfare threats. (4) What recommendations have been made regarding organizational means to address national IW strategic objectives., and (5) How might business process reengineering be applied to accomplishing a national IW strategy. To answer the above questions, this study discusses the roles and responsibilities of organizations currently involved in IW. The research then evaluates the problems areas associated with these current efforts and experts' recommended solutions. The thesis then recommends business process reengineering as an effective methodology for developing and implementing the needed national

policy. Specifically, the research provides a step-by-step process, based predominantly on Hyde's (1995) process management model, to utilize when pursuing this new national policy.
REPORT NUMBER: AFITGIRLAS97D1
ACCESSION NUMBER: ADA345731
http://handle.dtic.mil/100.2/ADA345731

Anderson, Emory A., Cynthia E. Irvine and Roger R. Schell. ***Subversion as a Threat in Information Warfare***. Charleston, SC: Space and Naval Warfare Systems Center North, 2004. 13p.
Abstract: *As adversaries develop Information Warfare capabilities, the threat of information system subversion presents a significant risk. System subversion will be defined and characterized as a warfare tool. Through recent security incidents, it is shown that means, motive, and opportunity exist for subversion, that this threat is real, and that it represents a significant vulnerability. Mitigation of the subversion threat touches the most fundamental aspect of the security problem: proving the absence of a malicious artifice. A constructive system engineering technique to mitigate the subversion threat is identified.*
ACCESSION NUMBER: ADA435312
http://handle.dtic.mil/100.2/ADA435312

Anderson, Robert H., et al. ***Securing the U.S. Defense Information Infrastructure: A Proposed Approach***. Santa Monica, CA: Rand Corporation, 1999. 179p.
Abstract: *This report addresses the survivability and assured availability of essential U.S. information infrastructures, especially when they are under various forms of 'information warfare' attack. To the best of our knowledge, the term 'minimum essential information infrastructure' (MEII) was coined by one of the authors (Mesic) as part of the planning for a series of 'Day After. in Cyberspace' information warfare exercises conducted from 1995 to the present under the direction of our RAND colleague Roger Molander. The idea is that some information infrastructures are so essential that they should be given special attention, perhaps in the form of special hardening, redundancy, rapid recovery, or other protection or recovery mechanisms. Players in the 'Day After' exercises were intrigued by the MEII concept but asked: Is this concept feasible. Is it practical. For what portions of the Department of Defense and U.S. infrastructure is the concept relevant. What would such infrastructures look like. How effective or useful would they be. This report documents the findings of the first year of a study of the MEII concept, attempting to formulate some initial answers to these questions-or, if these are not the right questions, to ask and answer better ones. This report should be of interest to persons responsible for assuring the reliability and availability of essential information systems throughout the U.S. defense establishment, the U.S. critical infrastructure, and other organizations. Its findings and recommendations are relevant at all organizational levels, from small units to major commands.*
REPORT NUMBER: RAND-MR-993-05D/NSA/DARPA
ACCESSION NUMBER: ADA365673
http://handle.dtic.mil/100.2/ADA365673

Ashman, Bruce W. ***Defensive Information Warfare in Today's Joint Operations: What's the Real Threat***. Carlisle Barracks, PA: Army War College, April 1997. 47p.
Abstract: *Information warfare (IW) is an emerging concept that affects the use of automated systems and reflects the growing realization that information technology can be used to gain an advantage over other users. Since the Gulf War, the incidents of information systems attacks have increased, especially in the civilian environment. Attacks against military systems have gone as far as penetrating sensitive, previously secure systems. As this threat against information or computer-based systems becomes more blatant, it raises the question of how vulnerable to attack are our automated military systems. Emerging technologies promise greater speed, accuracy and reliability for military operations while simultaneously producing greater lethality and situation awareness. However, as the Armed Forces depend more and more on these systems to perform routine and specialized operations, the risk of penetration, disruption,*

or even compromise becomes apparent. While information warfare has great potential as a valid offensive tool, this paper explores the threat to unified and joint military operations from a defensive information warfare perspective. We must first identify what the threat entails and design defensive procedures because this is where the greatest vulnerabilities lie. Research and development of IW as an offensive weapon can be pursued and funded along with other conventional weapons programs. What is critical is identifying weaknesses and correcting them before we become victims of information warfare itself.

ACCESSION NUMBER: ADA326368

http://handle.dtic.mil/100.2/ADA326368

Barac, Gregory G. ***Interoperability: The Cornerstone of Information Warfare***. Carlisle Barracks, PA: Army War College, April 1996. 27p.

Abstract: Information warfare has won the joint acceptance within DoD and may become the biggest threat faced by our nation. The great achievement of interoperability between information-based systems (e.g., computers) also introduced inherent risks and vulnerabilities, which is the cornerstone of information warfare. Information warfare includes the ability to exploit and dominate information made assessable through computers and communications. Should there be concern about these vulnerabilities. Absolutely. Modern societies depend upon these information-based systems to live and work. This paper introduces the recentness of information warfare and highlights some current issues, like who is leading the effort. The success of the information society to make their systems interoperate with other systems greatly increased the potentiality of information warfare. A review of the evolution of system interoperability highlights this phenomenon. As a result of being directly influenced by the industrial-age society, leaders over the age of forty may be too challenged to adequately grasp the issues of information warfare and may lead ineffectively.

ACCESSION NUMBER: ADA312146

http://handle.dtic.mil/100.2/ADA312146

Bennett, Sheila G. ***A Process for Vectoring Offensive Information Warfare as a Primary Weapon Option Within the United States Air Force***. Wright-Patterson AFB, OH: Air Force Institute of Technology, 2001. 150p.

Abstract: Consistently and comprehensively using Information Operations (IO) capabilities as a primary weapon option within the Air Force is the next step to operationalizing IO within the Air Force. Doctrine and official guidance have set the variables of mission and concepts of operations, organizational structure, and IW players in place. The missing variable to operationalizing IO and probably the most difficult is the "how" or process of the equation. This research will introduce a useable process that can be incorporated within the Air Force for integrating offensive IW activities into the current and given environment. The process is the basis for further decomposition and identification of target aim points. In addition, its use of effect points should aid in focusing long-range, deliberate, and crisis action planning on the possible desired effects on an adversary. The research sets the stage by briefly defining the first three variables; organization, mission, and players in which AF IW is practiced and the inherent deliverables required. It will then introduce a view and decomposition of the information battiespace as the basis for offensive IW activities where affecting the information factors in order to induce a desired decision to achieve desired effects is the overall goal.

https://research.maxwell.af.mil/viewabstract.aspx?id=2607

Black, Bruce J. ***Modeling Organizational Configuration and Decision Processes for Information Warfare Analysis***. Monterey, CA: Naval Postgraduate School, March 1997. 142p.

Abstract: For an organization to survive it must be able to adapt to its environment. A military organization operates in an environment that is constantly changing. The ability to model organizational configurations and organizational decision processes can assist the commander in adapting to the environment and understanding how a military organization is susceptible to Information Warfare (IW)

attacks. First a commander must understand the concepts of Information Warfare, Command and Control and the concept of organizational decision processes and how these permit an organization to adapt to its environment. Then the commander must determine what level of detail is necessary to model the organizational decision processes for its environment. Next the commander must analyze his model for configuration and decision processes. Using such commercially available software as Organizational Consultant and vDT the commander can identify any organizational misfits to the environment and the IW attack susceptibilities of the organizational decision processes. In the end, this approach demonstrates that it is feasible to model organizational configuration and organizational decision processes in an Information Warfare environment.

ACCESSION NUMBER: ADA333373

http://handle.dtic.mil/100.2/ADA333373

Boll, Kenneth. ***Like a Lightning Bolt - Information Warfare***. Carlisle Barracks, PA: Army War College, February 1999. 47p.

Abstract: *Combatant commanders currently do not have the best possible support from information warfare doctrine and capabilities that facilitate organizing forces for offensive and defensive information warfare. A balance of offensive and defensive information power is required and this research project suggests clearer doctrinal command and control relationships, integrated ways of employment, and sufficient information warfare means to enable a joint force commander to project dominant information power. The appropriate organization for combat will include a Joint Information Warfare Task Force to assist the joint force commander's planning effort and execute information operations.*

ACCESSION NUMBER: ADA364265

http://handle.dtic.mil/100.2/ADA364265

Braddock, Joseph V., et al. ***Concepts and Technologies for the Army Beyond 2010***. Washington, DC: Army Science Board, March 1999. 236p.

Abstract: *A study assessing the 2010-2025 timeframe and seeking technologies and enablers for Joint, Army and other Service operations with emphasis on Joint missions involving land combat. Specific areas of analysis include Mobility and Sustainment, Information Dominance, Platforms and Weapons and Investment Strategies. Study analyses suggest tapping commercial successes as private sector investment is strongly supporting improvements in many areas. However, to fully tap these developments the Army must begin participating in the design of future commercial systems. This study provides 9 major recommendations including: establishing an Investment Council, exploiting non-Army commercial capabilities, establishing a C4ISR testbed, and using FSCS vehicles as precursors for AA2010 platforms.*

ACCESSION NUMBER: ADA369372

http://handle.dtic.mil/100.2/ADA369372

Brand, John H., II. ***Proposed Modeling Protocol for Evaluating Information Attacks***. Aberdeen Proving Ground, MD: Army Research Laboratory, January 1999. 37p.

Abstract: *The essence of an information attack is to alter, either by intrusion into and manipulation of a database or by deception, the scenario under which a target mind or organization evaluates and selects future courses of action. The aim is to influence the actions of the target. The method is alteration of the perceived desirability or expected payoff of specific courses of action. This alteration of the information in possession of the target can be described as alteration of the perceived reality under which the target operates. Probable success by an attacker in altering the target's perceived behavior, given a successful manipulation of the target's information, has, in the past, been subjective. A modeling protocol based on the use of game theory is proposed that may, in certain cases, allow optimization of the scenario, or reality, imposed on the target to force the choice of a desired course of action. It should also allow a quantitative estimate of the likelihood of the target's adopting a given course of action. This tool can be used to estimate friendly susceptibility to information attack.*

REPORT NUMBER: ARL-TN-112

ACCESSION NUMBER: ADA362101
http://handle.dtic.mil/100.2/ADA362101

Bray, Clifton L., Jr. ***SCORPION: A Low Cost, Low Risk, Low Asset Strategy For Resolving Low Level Conflicts***. Carlisle Barracks, PA: Army War College, April 1996. 75p.

Abstract: Despite a significant drawdown, the U.S. military must be ready for two nearly simultaneous Major Regional Contingencies (MRCs). Frequent deployments in support of contingencies short of an MRC are affecting our MRC readiness. Often the cost for these large deployments comes from training, readiness, and modernization related funds. Deployed units cannot complete certain types of critical training and in some cases, lost training is never made up. Another problem is a rising concern toward casualties, especially casualties not clearly associated with America's vital interests. Is there a low cost, low risk, low asset strategy for resolving low level conflicts. This paper analyzes our current situation and proposes a strategy that combines precision guided munitions, stealth aircraft, information warfare, psychological operations, and unconventional warfare into an integrated method of fighting. This strategy is codenamed SCORPION.

ACCESSION NUMBER: ADA309113
http://handle.dtic.mil/100.2/ADA309113

Buchan, Glenn. ***Information War and the Air Force: Wave of the Future? Current Fad?*** Santa Monica, CA: Rand Corporation, March 1996. 16p.

Abstract: Information War, in all of its actual and semantic variations, is a very hot topic these days. The subject has received considerable attention in a variety of forums: serious analysis for professionals, popularized accounts for lay audiences, pop futurology, and post-Cold War melodramas. The national security bureaucracy is currently very active in this arena, with all of the military services and various civilian agencies and their supporting analytical organizations establishing centers for information warfare, writing position papers, and generally grappling with the problem of how to cope with the information revolution and its consequences. There is good news and bad news in the surge of interest in information warfare. The good news is that the public discussion could heighten the awareness of policy-makers to information-related issues and possibly help focus policy-level debates. Recognizing the importance of using information effectively in war is hardly news-Sun Tzu, for example, covered the subject over 2000 years ago. Moreover, there have been continuing, well established efforts in the national security community in many critical information-related areas electronic combat, computer and communications security, intelligence collection of all sorts, etc.-that long predate the current interest in information warfare.

ACCESSION NUMBER: ADA322532
http://www.rand.org/pubs/issue_papers/IP149/index.html

Burke, David A. ***Towards a Game Theory Model of Information Warfare.*** Wright-Patterson AFB, OH: Air Force Institute of Technology, November 1999. 116p.

Abstract: The repeated game of incomplete information model, a subclass of game theory models, was modified to include aspects of information warfare. The repeated game of incomplete information model was first developed to analyze nuclear weapons disarmament negotiations. The central role of information in this model suggested its applicability to IW, which focuses on the defense and acquisition of information. A randomized experimental design was utilized to determine how people behave in a laboratory IW setting and to test the IW game model's basic predictions. The impact of experience and learning on IW performance was also assessed during the experiment. IW experience and devices that support learning during an IW engagement improved performance in some situations. The IW game theory model was shown to have some predictive capability and, with further development, could support further IW analysis and simulation.

REPORT NUMBER: AFIT/GSS/LAL/99D-1
ACCESSION NUMBER: ADA374162

https://research.maxwell.af.mil/viewabstract.aspx?id=2251
http://handle.dtic.mil/100.2/ADA374162

Butler, Bradley L. ***Need for a USAF Information Warfare (IW) Strategy for Military Operations Other Than War (MOOTW).*** Maxwell AFB, AL: Air University, 1 April 1996. 65p.

Abstract: With the end of the Cold War, much has been written recently about the future direction the U.S. should take in an uncertain and rapidly changing world environment. The decision will have far reaching implications for many years to come. Two areas having an impact on the answer to this question but not normally examined together are information warfare and the broad area of military operations short of large scale conventional combat operations commonly known as military operations other than war (MOOTW) and very recently alluded to as other military operations (OMO). This paper examines both the information warfare environment and MOOTW to determine emerging information warfare technologies that may impact on MOOTW, as well as to determine those types of MOOTW requiring unique information warfare capabilities not currently planned for in large scale conventional warfighting operations. The limitations of using information warfare in MOOTW are also examined in some detail. The author contends that although emerging Air Force strategy and doctrine on information warfare should attempt to address MOOTW more than it currently does, in general strategy and doctrine will be subject to more constraints than corresponding information warfare strategy and doctrine for mid to high intensity conflict.

ACCESSION NUMBER: ADA330874
http://handle.dtic.mil/100.2/ADA330874

Cabral, Paul A. ***Information Warfare and Information Operations: Protecting The Global Information Environment.*** Carlisle Barracks, PA: Army War College, March 1998. 41p.

Abstract: The United States is an information and information systems dominated nation. Because of its dependence on information and information technology, the United States has become one of the most vulnerable nations to information warfare attacks. This study examines vulnerabilities in the global, national and defense information infrastructure and information operations attacks (information warfare) in the context of the national strategy for protecting the information infrastructure. It reviews directives, regulations, and policies currently in place to protect the information infrastructure and recommends the part government should play in this effort. It concludes with recommendations regarding a coordinated government and private sector office at the national level to provide the leadership required for such an effort.

ACCESSION NUMBER: ADA344848
http://handle.dtic.mil/100.2/ADA344848

Cardillo, Richard G., Jr. ***Fighting the 20th Century Army into the 21st Century***. Carlisle Barracks, PA: Army War College, April 1999. 45p.

Abstract: The Army of the future is undergoing a transformation from a forward deployed 'Cold War' army to a power projection force. This transition will eventually result in a fully digitized, more tailorable, rapidly expandable, strategically deployable, and effectively employable organization. Until this transformation is complete, it may require a change to our doctrine and to our tactics, techniques, and procedures on how we integrate digitized and non- digitized systems and organizations into the fight. This paper addresses those possible changes. To leverage the true power of the future battlefield, commanders and their staffs must have a clear understanding on the capabilities and limitations that these new systems possess. Our challenge and primary goal of America's Army in this process is to keep the preeminent war-fighting skills ready and relevant while the Army evolves into the world's premier 21st Century fighting force.

ACCESSION NUMBER: ADA364565

http://handle.dtic.mil/100.2/ADA364565

Carr, Thomas H. ***War on the Cheap. Using Information Warfare to Lengthen the Decision Cycle***. Newport, RI: Naval War College, February 1996. 27p.

Abstract: This paper investigates how an adversary of the United States might indirectly attack a center of gravity of a United States military operation by disrupting operational tempo using information warfare. Current military doctrine mandates quick and decisive victories whenever United States Forces are called to combat. A key element of this doctrine is the creation of an operational tempo that an enemy cannot match and so defeating him quickly with as few casualties as possible. The doctrine reflects a political reality that the American public will not support protracted and indecisive conflicts with large numbers of casualties. It is also a fact that most future United States military operations will project forward from the continental United States to immature theaters of operations. The combination of the requirements for high operational tempo and power projection from the United States will demand much from our information technology. Automated support systems for administration and logistics will be key to any future successful operation. This paper will not discuss how information resources are used by the United States but rather how a potential adversary might be able to manipulate these resources to disrupt operational tempo. This paper will show how a financially limited country could effectively fight the United States military, not by buying expensive exotic weapons systems, but by paying talented computer hackers and others familiar with United States support networks to disturb these systems. A good information warfare capability such as this would be a great combat multiplier for any foe and is not a capability realized sufficiently by United States military joint planners.

ACCESSION NUMBER: ADA307767

http://handle.dtic.mil/100.2/ADA307767

Carter, Rosemary M. ***Army Information Centers of Gravity: Can We Protect Them***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1999. 62p.

Abstract: As the Army keeps pace with the information age, it must determine how to leverage information to win its wars. According to Brigadier General Wayne M. Hall information is a tool for influencing an enemy's decision cycles. This is achieved by attacking the enemy's information centers of gravity. BG hall defines these information centers of gravity as the physical place or mental construct in cyberspace where a confluence of intellect, decisions, collection, automation, communications and planning occurs. The purpose of this monograph is to determine if the U.S. Army has information centers of gravity and if so, can they be protected. The monograph first determined the key components of information from the definition of information superiority. These key components were analyzed using three criteria to determine the Army's information centers of gravity. The criteria used were their influence on decision cycles, effects on strategic aims, and impact on combat power. The analysis concluded that there are two information centers of gravity Army commanders and information operations cells. The monograph used the Army's defensive IO capabilities to determine if it can protect these information centers of gravity. The conclusion is that the U.S. Army does have the capability to provide protection for these information centers of gravity. The monograph concluded with a look at additional initiatives that are ongoing to protect both information centers of gravity and the key components of information that support these centers.

ACCESSION NUMBER: ADA370329

http://handle.dtic.mil/100.2/ADA370329

Chaturvedi, A. R., et al. Agent-Based Simulation Approach to Information Warfare in the SEAS environment." p. 32, IN: ***System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference***, January 4-7, 2000.

Abstract: Not available.

Clark, Howard W. and Saundra K. Wallfesh. ***Measuring Effectiveness of Theater IW/C2W Campaigns***. Wilmington, MA: Dynamics Research Corporation, April 1995. 20p.

Abstract: This effort, which addresses measures of effectiveness for theater operations, is a continuing commentary on how the senior commander of a military operation pulls all these things together and how IW and Command and Control Warfare (C2W) supports the theater campaign. The paper first establishes some groundwork in the Background section, which presents the concepts of theaters, levels of war, levels of command, OOTW, and sources. Next, IW and C2W are discussed. The Measurement section examines the concept of measuring, looking at what, when, how to measure, and subjective versus objective measures. Examples of theater level measures of effectiveness (MOEs) are provided in the following section, Theater MOE, in which the Theater Level MOE Worksheet is introduced. Modeling is addressed in the next section, which states why models are of interest, suggests improvements, and discusses worksheet applicability. Finally, we present suggestions for improving the measurement of theater level C2W. It is our intent to provide, for policy makers as well as commanders, some techniques for them to measure the effectiveness of their campaigns and operations.

ACCESSION NUMBER: ADA330423

http://handle.dtic.mil/100.2/ADA330423

Clements, Stacy M. ***One With the Most Information Wins: The Quest for Information Superiority***. Wright-Patterson AFB: Air Force Institute of Technology, OH. School of Logistics and Acquisition Management, December 1997. 140p.

Abstract: The escalation of interest in information as a corporate resource is reflected in the military's quest for information superiority. A volume of directives, articles, and doctrine is appearing to meet the unique challenges presented by information as a resource. Discussions of how to achieve information superiority have given rise to investigations of such related concepts as information warfare and information operations, with associated taxonomies and ideas of how to use information capabilities for attack and defense. This thesis examines information superiority and the related concepts, and examines current information technology initiatives in order to discern the characteristics which can aid in the quest for information superiority. A synthesis of the most prominent perspectives on information superiority is formed. In the context of this definition, a process model of information superiority and its necessary activities is developed, with acquisition and decision making identified as key. The idea of information technology as enabling information superiority is probed, and an alternate view proposed; contending that information technology is more likely to be detrimental to information superiority unless certain criteria are met. The resulting conceptual model depicts the key attributes of information superiority and information technology, and represents the relationships between these concepts.

ACCESSION NUMBER: ADA335235

https://research.maxwell.af.mil/viewabstract.aspx?id=1170

http://handle.dtic.mil/100.2/ADA335235

Collier, Mark. ***Information Warfare Modeling I***. San Antonio, TX: Southwest Research Institute, October 1997. 46p.

Abstract: This report documents the results of survey task in which the contractor was asked to identify current Information Warfare (IW) modeling development within the Department of Defense (DoD) and recommend an approach for IW modeling. It involved working with Rome Laboratory to identify their primary interest area in IW Modeling, surveying DoD for ongoing unclassified IW modeling efforts, and defining an IW modeling architecture which Rome Laboratory could use in the future to guide research and development.

REPORT NUMBER: RLTR97176

ACCESSION NUMBER: ADA337178

http://handle.dtic.mil/100.2/ADA337178

Cook, Wyatt C. ***Information Warfare: A New Dimension in the Application of Air and Space Power***. Maxwell AFB, AL: Air War College, 1994. 38p.

Abstract: The emergence of information warfare and its application to air and space doctrine will forever change the form and conduct of modern warfare. While history does not provide specific solutions that can be applied without modification to present and future situations, it does provide a broad conceptual basis for understanding war, human nature, and air and space power. This document provides the framework for exercising judgement and is a starting point for understanding what information warfare is and hit it can be applied. Like any doctrine, information warfare doctrine should be alive--growing, evolving, and maturing. New experiences, reinterpretation of past experiences, advances in technology, changes in threats and cultures can (and should) require alternation of doctrine. We must leverage and maximize the advantage of technology to harness the benefits of the information technology explosion, if we are to win the information war.

ACCESSION: ADA280804

Cooney, David M., Jr. ***Warfare in the Information Age: Adding Capability Multipliers***. Newport, RI: Naval War College, Joint Military Operations Department, May 1999. 25p.

Abstract: One recurring theme in military writings since the end of Desert Storm is that the American military is on the cusp of a new Revolution in Military Affairs (RMA). Proponents of this viewpoint cite major changes in business and society brought on by the personal computer and the Internet. They view these changes as part of a new information age and predict that the explosive technological growth in the speed of microprocessors and networks will lead to whole new ways to wage war, with information superiority being the key ingredient to assure victory. Critics argue that war as a rough, brutish, and frequently irrational business, and that no network will eliminate either the fog or friction of war. They see many of concepts being put forward as not respectful of the enduring principles of war. This paper argues that regardless of whether revolutionary changes occur in the way wars are fought in the information age or whether developments will continue to follow a more evolutionary path, - the military needs to look beyond technology and begin the process of accelerating its ability to assimilate the changes technology brings. This paper presents five capability multipliers for warfare in the information age: (1) assembling and maintaining the intellectual capital to operate in the future networks; (2) developing information as a true discipline; (3) improving human computer interaction; (4) seeking greater understanding of how people process information and make decisions; and (5) furthering the cultural, organizational, and operational concepts to support the technological change.

ACCESSION NUMBER: ADA370707

http://handle.dtic.mil/100.2/ADA370707

Cooper, Jeffrey R. ***Another View of the Revolution in Military Affairs***. Carlisle Barracks, PA: Army War College, Strategic Studies Institute, July 1994. 57p.

Abstract: The author urges defense planners to determine what strategic--as opposed to operational--benefits might be derived from the Revolution in Military Affairs (RMA). He cautions against being so focused on the technology of the RMA as to divert attention from the critical relationships between purpose, strategy, doctrine, operational innovation and organizational adaptation. He concludes that making the internal reforms that will be required will be as challenging as coming to terms with the operational and strategic implications of the new technologies.

ACCESSION NUMBER: ADA283587

http://handle.dtic.mil/100.2/ADA283587

Cramer, Michael J., Sowmya Ramachandran, and Janelle K. Viera. **Using Computer Games to Train Information Warfare Teams**. San Mateo, CA: Stottler Henke Associates, Inc., 2004. 11p.

Abstract: Information warfare and security are crucial to maintaining homeland security. An important mission of the information warfare force is to ensure that secure information and facilities are well protected. One way to ensure this is to try to gain access to this information as outsiders and see how well the practices and policies designed to protect data are being enforced. Teams of Information Warfare personnel (a.k.a. the Red Teams) are dedicated to the mission of testing the security of information and assets crucial to American interests. Most such missions necessitate deception in order to test the extent to which data is protected from strangers and parties who are not trusted. High-levels of stress are inevitable, and the Red Teams need to be highly skilled in thinking creatively under such stress. Given the criticality and the degree of danger of these missions, they have to be carefully trained. For computer-based approaches, providing realistic simulations is essential for successful training. Engaging the trainee emotionally to elicit the types of stress responses they will experience on real missions is crucial. 3D computer games have proved themselves to be highly effective in engaging players motivationally and emotionally. This effort, therefore, uses gaming technology to provide realistic simulations. These games are augmented with Artificial Intelligence techniques for enabling trainees to interact with the simulation using natural language, intelligent evaluation of the student's performance, and automated after-action review that allows the trainees to assess their own performance and provide justifications for their actions. This paper describes the details of this approach, providing examples of the simulations and after-action reviews, and discusses its benefits and limitations.

ACCESSION NUMBER: ADA459676

http://handle.dtic.mil/100.2/ADA459676

Crawford, George A. ***Information Warfare: New Roles for Information Systems in Military Operations***. Washington, DC: Department of the Air Force, December 1997. 20p.

Abstract: Information warfare (IW) theory has tremendous political, technical, operational, and legal implications for the military. This article seeks to define IW for the layman and discuss its potential applications. It also attempts to identify potential military uses of existing information systems technology and address some of the issues facing those who will be responsible for implementing this new doctrine.

ACCESSION NUMBER: ADA332446

http://handle.dtic.mil/100.2/ADA332446

Crew, Benjamin F. ***Information Warfare, Organizing for Action***. Newport, RI: Naval War College, June 1996. 32p.

Abstract: The armed forces of the United States have recognized the potential importance of Information Warfare (IW) and have defined it as it will apply to military operations. It now remains for them to identify and implement an optimum organizational structure at the regional unified command level to develop, plan, synchronize and employ it effectively. Official publications recommend an 'IW cell' made up members from the J3, J6 and J2 directorates of the CINCs staff. Any such organization needs unity of command, unity of effort and uniformity between the commands to succeed. Alternative organizational structures include a separate staff element, a single DoD Agency or service in charge, or a new functional unified combatant command--USINFOCOM. Although none of the organizations offers a solution that is totally acceptable, USINFOCOM may be the best alternative. That solution can only be implemented, however, after careful consideration of the way in which IW is to be viewed--as a force multiplier or as a form of warfare, and then only after today's warriors become acculturated to the phenomenon of IW.

ACCESSION NUMBER: ADA312020

http://handle.dtic.mil/100.2/ADA312020

Curts, Raymond, J. and Douglas E. Campbell. ***Command & Control as an Operational Function of Information Warfare.*** Fairfax Station, VA: Strategic Consulting Inc., 2004. 33p.

Abstract: *Data - the competition for information is as old as the first conflict. It involves increasing and protecting our own store of information while limiting and penetrating the adversary's. As it pertains to C2 as an operational function of information warfare - targeting the enemy's information functions, while protecting ours, with the intent of degrading his will or capability to fight. Management e.g., advanced battlefield management (e.g., using information and information systems to provide information on which to base military decisions when prosecuting a war); and Risk Management for the risks potentially associated with information and information technology (IT) to be identified and managed cost effectively, it is essential that the process of analyzing and assessing risk is well understood by all parties and executed on a timely basis. Process - Information Warfare processes are making dramatic changes in how we fight wars. The process must allow a commander's vision and view of the battlespace to be shared at the lowest possible level. From the unique perspectives of soldiers, sailors, marines and airmen, the process must forge a common understanding of how to use information warfare to enhance joint C2 warfighting capabilities. The Global Information Grid (GIG) is an example of such a process.*

ACCESSION NUMBER: ADA465787

http://handle.dtic.mil/100.2/ADA465787

Denno, Patricia. ***Defense Information Warfare Technology Applications (DIWTA) Automated Intrusion Detection Environment (AIDE) Advanced Concept Technology Demonstration (ACTD).*** McLean, VA: Northrup Grumman Technology Defense Enterprise Solutions, 2004. 63p.

Abstract: This report represents work done in Task 0001 and Task 0008. This paper is organized into the three years represented. Introductory material provides an overview. Subsequent sections for each year begin by describing the development process which was based on incorporating the lessons learned from the previous year, the goals for the year, and including innovations from AFRL. The paper then describes for each year the deployment and demonstration planning processes. Demonstration performance is described and summary data from each year's demonstration follows. Finally user feedback and hot wash conclusions are then presented by year, leading to a discussion of suggested improvements for Year Three development. A final conclusions section completes the document.

ACCESSION NUMBER: ADA429896

http://handle.dtic.mil/100.2/ADA429896

DeVries, Anita D. ***Information Warfare and Its Impact on National Security***. Newport, RI: Naval War College, June 1997. 20p.

Abstract: For years, the United States national security posture has relied heavily on secured sea lines of communication, friendly borders, unmatched human and material resources, unlimited mobilization capability, and nuclear hegemony. This paper defines information warfare; examines its offensive and defensive components; explores potential threats, information warfare legalities and nature; and concludes that we face a tremendous challenge at the strategic level to keep our current status of being a world power to be reckoned with.

ACCESSION NUMBER: ADA325003

http://handle.dtic.mil/100.2/ADA325003

Dick, Samuel R. ***Operational Proponent for Information Warfare***. Newport, RI: Naval War College, Joint Military Operations Department, June 1996. 24p.

Abstract: How Information Warfare is integrated into the Commander in Chief and Joint Task Force staffs will determine its successful application in wartime. Three criteria are formulated: (1) inter-agency participation, (2) national approval for operations, and (3) a long-term studies program. Three models are analyzed: (1) Command and Control Warfare cell, (2)Joint Psychological Operations Task Force, and (3)

Special Operations Component. The most suitable choice using the three criteria is to establish an Information Warfare organization similar to the Joint Psychological Operations Task Force.
ACCESSION NUMBER: ADA311989
http://handle.dtic.mil/100.2/ADA311989

Dishong, Donald J. ***Studying the Effect of Information Warfare on C2 Decision Making***. Monterey, CA: Naval Postgraduate School, June 1994. 61p.
Abstract: The goal of practitioners of information warfare is always concerned with affecting the decisions made by the enemy. With a clear understanding of how the enemy makes decisions, it is easier to target the processes which are involved in making those decisions. The purpose of this thesis is to demonstrate whether information warfare, when directed at a command and control decision maker, can be administered in quantified amounts which can be used to change what would normally be a good tactical decision into a bad one. This thesis uses a software package called Tactical Tic-Tac-Toe (T4), to simulate command and control decisions being made in an information warfare environment. The three measures of effectiveness of winning battles, winning missions (aggregate battles), and increasing one's won-to-loss ratio are used to evaluate the quality of the decisions being made. Fog of War, Tactical Delay, Area Delay, and Communications Delays are combined to determine their effects on command and control under these measures of effectiveness. Clearly the data shows that delaying one's immediate opponent from grasping the tactical picture serves to greatly enhance the chances of increasing one's effectiveness. Further, delaying the enemy's understanding of 'pieces' of the strategic picture (which might not be viewed as immediately tactically important), also dramatically increases effectiveness.
ACCESSION NUMBER: ADA283639
http://handle.dtic.mil/100.2/ADA283639

Dockery, J. T. and A. E. R. Woodcock. "'Crisis Mind' Versus 'Combat Mind.'" p. 1120-1124, IN: ***Military Communications Conference, 1995. MILCOM '95***, Conference Record, IEEE, 5-8 November 1995, 1291p.
Abstract: This paper is about modelling information warfare and its effect on simulated command and control. In it we introduce a new perspective based on the arguable difference between decision making during a (possibly extended) crisis and that occurring during combat. Our subject is the commander's mind set. For this purpose we distinguish what we call a crisis mindset and a combat mindset. Each is to be evaluated by the nature of the response which the commander chooses. While it is true that combat may be thought of as one long crisis, we make a distinction between a crisis situation and a combat situation. Our purpose is to better incorporate human command decision making into simulations. Only them can the effects of information warfare be reliably predicted.

Downs, Lawrence G., Jr. ***Digital Data Warfare: Using Malicious Computer Code as a Weapon***. Maxwell AFB, AL: Air University, Air War College, April 1995. 38p.
Abstract: Digital Data Warfare (DDW) is an emerging field that has great potential as a means to meet military, political, economic or personal objectives. Distinguished from the 'hacker' variety of malicious computer code by its predictable nature and the ability to target specific systems, DDW provides the attacker with the means to deny, degrade, deceive and/or exploit a targeted system. The five phases of a DDW attack -- penetration, propagation, dormancy, execution and termination -- are presented for the first time by the author in this paper. The nature of DDW allows it to be used in the strategic, operational and tactical warfare roles. Three questions should be considered when developing a strategy for employing DDW: (1) Who should control the employment of DDW. (2) What type of systems should be targeted, and (3) Under what circumstances should DDW be used. Finally, a brief overview of possible countermeasures against DDW is provided as well as an outline of an effective information system security program that would provide a defense against DDW.
ACCESSION NUMBER: ADA328638
https://research.maxwell.af.mil/viewabstract.aspx?id=1623
https://research.maxwell.af.mil/papers/ay1995/awc/downslg.pdf

Elam, Donald E. ***Attacking the Infrastructure: Exploring Potential Uses of Offensive Information Warfare***. Monterey, CA: Naval Postgraduate School, June 1996. 216p.

Abstract: The world has entered the Third Wave; it has entered the Information Age. One of the fundamentals of this paradigm shift is the fact that information is power. The side that controls information more effectively will be victorious. Thus, countries and militaries must change their mentality in order to survive. A new form of conflict, Information Warfare, has been born. This new discipline is large, dynamic, and complex. The need exists for education among military officers and other concerned professionals throughout the country. This thesis helps to bridge the education gap. It presents a snapshot of Information Warfare today, exploring many different avenues and possibilities along the way. The first half of the document is focused on Information Warfare in general, and the second half deals specifically with the offensive side. The purpose of this thesis is not to present an all-encompassing view of Offensive Information War or eve of Information Warfare in general. The field of Information Warfare is too big for any one individual or organization to fully comprehend all of its intricacies. Indeed, due to the dynamic nature of this discipline, chances are that some, or maybe even all, of the material contained herein will be obsolescent upon publication. The goal of the thesis is to present one view of Information Warfare, as seen through the eyes of many. The hope is that some benefit will be garnered by the reader, even if it only sparks an idea or helps to understand the importance of this growing warfare dimension.

ACCESSION NUMBER: ADA311391

http://handle.dtic.mil/100.2/ADA311391

Englin, David L. ***Lightning Bolt and the Quill: Determining the Role of Air Force Public Affairs in Information Warfare***. Cambridge, MA: Harvard University, October 1998. 50p.

Abstract: As the Air Force's internal and external public voice, Air Force public affairs is uniquely positioned to influence the flow of information to different audiences about a variety of issues and operations. In this new operating environment, Air Force public affairs must determine its proper role in information warfare. The key to determining this role is to examine the tension between the public information and public relations functions of Air Force public affairs. The public information function focuses on the complete release of all information about the Air Force. The public relations function focuses on influencing public opinion to benefit the Air Force. A survey of documents defining the mission of public affairs suggests conflicting views within the US military concerning the public information and public relations functions. Department of Defense and Joint Staff documents define the mission of public affairs strictly in terms of public information, and even prohibit some public relations activities. Air Force documents define the mission of public affairs in terms of both public information and public relations, permitting the use of accurate, honest public information to perform public relations. Moreover, the Air Force public affairs core competencies (Trusted Counsel to Leaders, Airman Morale and Readiness, Public Trust and Support, Global Influence and Deterrence) identify several important public relations activities. Several Department of Defense and Joint Staff documents explicitly constrain the potential information warfare role of Air Force public affairs. The following list of constraints emerges from these publications: (1) Quickly and completely release all information. (2) Never release any kind of misinformation. (3) The only valid reasons for restricting or withholding information are national or operational security and the safety and privacy.

ACCESSION NUMBER: ADA358580

http://handle.dtic.mil/100.2/ADA358580

Feiring, Douglas I. ***Information Warfare...From the Sea. Integrating Information Operations and the Marine Corps Planning Process.*** Quantico, CA: Marine Corps Command and Staff College, 2001. 12p.

Abstract: Although the Marine Corps's current method of planning and employing Information Operations (IO) seeks to integrate its various elements, improvements must be made for this emerging concept to be a truly effective force multiplier.

ACCESSION NUMBER: ADA400017

http://handle.dtic.mil/100.2/ADA400017

Ferguson, Robyn E. ***Information Warfare with Chinese Characteristics: China's Future View of Information Warfare and Strategic Culture***. Fort Leavenworth, KS: Army Command and Staff College, 2002. 68p.

Abstract: The Information Age presents a unique opportunity to China with regard to both modernization and building an Information Warfare (IW) capability. China's active pursuit of an IW capability will cause a change in Chinese strategic culture. According to Alastair Iain Johnston, strategic culture defines how a nation assesses a threat to its interests and whether it will use force to deal with those threats. The author's original research question asked how Chinese strategic culture will affect the development of a Chinese IW capability. The author answers that question by defining IW from American and Chinese perspectives and defining Chinese strategic culture, and then describes key aspects of People s Liberation Army (PLA) theorists vision for IW. The conclusion of this thesis is that the nature of cyberspace, the futility of the static defense, and the interdependence of the defense and the offense will change some aspects of Chinese strategic culture. This finding is contrary to the expected outcome, as the original research question anticipated that Chinese strategic culture would affect the development of a Chinese IW capability.

ACCESSION NUMBER: ADA416897

http://handle.dtic.mil/100.2/ADA416897

Fields, Gregory S. ***The Effects of External Safeguards on Human-Information System Trust in an Information Warfare Environment***. Wright-Patterson AFB, OH: Air Force Institute of Technology, 2001. 150p.

Abstract: This research looks at how human trust in an information system is influenced by external safeguards in an Information Warfare (IW) domain. The military command and control environment requires decision-makers to make tactical judgments based on complex and conflicting information received from various sources such as automated information systems. Information systems are relied upon in command and control environments to provide fast and reliable information to the decision-makers. The degree of reliance placed in these systems by the decision-makers suggests a significant level of trust. Understanding this trust relationship and what effects it has on the focus of this study. A model is proposed that predicts behavior associated with human trust in information systems. It is hypothesized that a decision-maker's belief in the effectiveness of external safeguards will positively influence a decision-maker's trusting behavior. Likewise, the presence of an Information Warfare attack will have a negative affect a decision-maker's trusting behavior. Two experiments were conducted in which the perceived effectiveness of external safeguards and the information provided by an information system were manipulated in order to test the hypotheses presented in this study. The findings from both experiments suggest that a person's trust computers in specific situations are useful in predicting trusting behavior, external safeguards have a negative effect on trusting behavior, and that Information Warfare attacks have no effect on trusting behavior.

ACCESSION NUMBER: ADA394373

http://handle.dtic.mil/100.2/ADA394373

https://research.maxwell.af.mil/viewabstract.aspx?id=3635

Franklin, Derek L. ***Information Warfare: Issues Associated With the Defense of DOD Computers and Computer Networks.*** Quantico, VA: Marine Corps Command and Staff College, 2002. 62p.

Abstract: The threat to the Defense Information Infrastructure is growing Hackers have advanced in sophistication and the potential exists for an alliance of independent hackers and terrorist/criminal groups that may threaten the critical information pathways of the armed forces An analysis of the history of computer information warfare reveals that there was an embarrassing lack of readiness and defense capability available to the armed forces of the United States before 1999. With the establishment of the Joint Task Force-Computer Network Defense (JTF-CNO) later renamed to Computer Network Operations in 1998 (JTF-CNO), a minimum capacity to respond has been developed However, as the issue has grown in importance, policy makers and planners have come to realize the limitations of Computer Network Attack (CNA) and Computer Network Defense (CND) as warfare areas The growth of related legal and law enforcement issues, and the effect of a possible enemy CNA strike, will require the coordination of civilian, armed forces, and law enforcement officials to respond effectively This will prevent CNA/CND from being a purely military issue.

ACCESSION NUMBER: ADA404740

http://handle.dtic.mil/100.2/ADA404740

Franz, George J. ***Information --The Fifth Element of Combat Power***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1996. 74p.

Abstract: This monograph proposes that one of the Army's primary doctrinal concepts, combat power, requires modification to keep pace with the changing environment of conflict. It argues that the Army's combat power model, defined as the combined effects of maneuver, firepower, protection, and leadership, represents one element of the Army's foundation that must be updated to meet the requirements of modern warfare. The current combat power model fails to recognize the impact that the current Revolution in Military Affairs, specifically embodied in the emergence of information operations, has on today's Army and will have on the Army of the future. The monograph examines emerging information operations (IO) doctrine contained in FM 100-5 Operations, FM 100-6 Information Operations, TRADOC Pamphlet 525-5 Force XXI Operations--A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, and related publications. It analyzes the current model and defines the integral elements of combat power and the conditions that affect their application. In turn, the study identifies the current elements of combat power that are included in information warfare (IW) and distinguishes those aspects of 10 not imbedded in the current combat power model. Detailing the components of IW and surveying current Army doctrine regarding information operations builds a foundation for examining the historical case study and for examining proposed future doctrine. A historical case study of Operation DESERT STORM provides the groundwork for considering the role information plays in the current combat power model. The analysis of the contemporary paradigm and the historical examination of IO combined with an overview of emerging concepts developed to support Force XXI affords a thorough basis for establishing a new framework.

ACCESSION NUMBER: ADA314297

http://handle.dtic.mil/100.2/ADA314297

French, Geoffrey S. ***Rethinking Defensive Information Warfare*.** Oakton, VA: General Dynamics, 2004. 47p.

Abstract: Although the origins of information warfare lie in the defense of critical computer systems, defensive information warfare (DIW) per se has advanced little beyond an information assurance model. Information assurance is an integral part of any military organization's operations, but it falls far short of meeting the needs for robust defense of critical command-and-control (C2) computer networks against a sophisticated adversary. By looking at the ways that militaries have responded to challenging defensive situations in the past, some insights can be made into the nature of IW and potential application of conventional operations. This paper examines defensive tactics and strategies from the German defense

in depth that emerged from World War I to the American Active Defense that developed in the Cold War and proposes a new mindset for DIW that draws on these operational concepts from military history.
ACCESSION NUMBER: ADA 465836
http://handle.dtic.mil/100.2/ADA465836

Gauthier, Kathryn L. ***China as Peer Competitor? Trends in Nuclear Weapons, Space, and Information Warfare***. Maxwell AFB, AL: Air University, Air War College, July 1999. 45p.
Abstract: In China as Peer Competitor. Trends in Nuclear Weapons, Space, and Information Warfare Lt Col Kathryn L. Gauthier analyzes the potential for China to emerge as a peer competitor of the United States in the coming decades. First, she examines two traditional pillars of national strength--China's status as a nuclear weapons state and as a space power. Second, she then explores China's growing focus on information warfare (IW) as a means to wage asymmetric warfare against a technologically advanced adversary. Third, the author carefully examines the status of the three programs highlights areas of concern and potential conflict with the United States, and analyzes the implications of these issues for the United States.
ACCESSION NUMBER: ADA367983
https://research.maxwell.af.mil/viewabstract.aspx?id=418
http://handle.dtic.mil/100.2/ADA367983

Gilliam, Mary M. ***Information Warfare: Combating the Threat in the 21st Century***. Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 52p.
Abstract: As we approach the dawn of the 21st century, success of our national security strategy will depend greatly on our ability to combat the Information Warfare (IW) threat. Old paradigms regarding conventional warfare must change to incorporate this new form of warfare. Our nation's growing dependency on information and information-based technologies has made IW a legitimate weapon for potential adversaries. The "information" and its support infrastructures are becoming extremely vulnerable to hostile attacks. Adversarial forces can now wage information-based warfare from anywhere in the world, and literally remain anonymous. Thus, our ability to recognize and defend against this new form of warfare is paramount to the survival of our national security infrastructure. The thesis of this research project is predicated upon the following premises: First, the exploitation of "information" as a weapon is changing the nature of warfare. Second, although there is much debate about the reality of the IW threat, this paper postulates that adversarial IW tactics pose a legitimate threat to our national security infrastructure. Finally, the Department of Defense (DOD), the Joint Staff, and the Services must remain actively committed to combating the IW threat in the 21st century.
ACCESSION NUMBER: ADA397986
http://handle.dtic.mil/100.2/ADA397986
https://research.maxwell.af.mil/viewabstract.aspx?id=1122

Ginn, Patrick W. ***Correlation Analysis of Fleet Information Warfare Center Network Incidents***. Monterey, CA: Naval Postgraduate School, 2001. 53p.
Abstract: The Navy's Intrusion Detection process is currently reactive in nature. It is designed and programmed to detect and provide alerts to the Fleet Information
Warfare Center (FIWC) of suspicious network activity while it is in progress, as well as to record/store data for future reference. However, the majority of activity taking place within and across Naval networks is legitimate and not an unauthorized activity. To allow for efficient access and utilization of the information systems sharing the network the Intrusion Detection Systems must be set at a level that filters out activity deemed as normal or non-hostile, whilestill providing an appropriate level of security. With this filtering in place an IDS system will not register all suspicious activity, and may not detect mild and seemingly harmless activity. When increasing security, limits must be imposed upon access*. This thesis examines FIWC network incident data from 1999 to see if a correlation can be drawn between United States visibility in the foreign media during 1999 and the occurrence of suspicious network incidents. A*

positive correlation may provide advance-warning indicators that could lead to the development of a procedure for increasing security posture based on the current environment. These indicators would provide a more proactive method of defense, significantly reduce potential damage caused by hostile network incidents and provide for more efficient network activity.

ACCESSION NUMBER: ADA396275

http://handle.dtic.mil/100.2/ADA396275

Guthrie, Samuel A. ***Knowledge-Based Operations: The 'So What' of Information Warfare*.** Fort Leavenworth, KS: Army Command and General Staff College, April 1995. 59p.

Abstract: After publishing the Army's centerpiece doctrinal manual FM100-5 Operations in June 1993, the Army lived up to its assertion that intellectual change leads physical change and immediately began working on its vision of future joint military operations. This vision, referred to as Force XX1 Operations, lays a conceptual foundation for military operations in the 21st century. This monograph explores a part of the future vision referred to as Knowledge-Based Operations. Battlefield frameworks have evolved over time providing a useful construct to guide preparation for the nation's next war. TRADOC Pamphlet 525-5 introduces a knowledge-based battlefield framework. This framework promotes the battle commander's ability to visualize the employment of forces and resources to dominate operational tempo. Within this framework the US Army proposes to achieve a decisive edge through the conduct of Knowledge-Based Operations. This monograph traces the evolution in battlefield frameworks, describes the knowledge-based framework, and presents a concept for Knowledge-Based Operations. This concept is the heart of the - monograph. The potential impacts of the new framework and Knowledge-Based Operations on campaign and joint operations planning are discussed and conclusions are presented. Elements of the battle dynamics are used for evaluation criteria throughout.

ACCESSION NUMBER: ADA300210

http://handle.dtic.mil/100.2/ADA300210

Hall, Larry P. ***National Military Strategy: Information Warfare***. Carlisle Barracks, PA: Army War College, April 1997. 33p.

Abstract: The U. S. Government has realized that new technologies will have a significant impact not only on everyday life but also on national security and the conduct of future warfare. While evaluating the powerful potential of information, policymakers are also attempting to understand a variety of problems surrounding it. This paper analyzes IW, specifically the protection of information, as a component of the 1995 National Military Strategy (NMS). It reviews the ends, ways, and means of our IW strategy. It focuses on the actions of the U. S. Government, the Department of Defense (DoD), and Joint Chiefs of Staff (JCS), especially on the U. S. Army's role. It examines the Army's IW strategy and provides some recommendations for what it needs to do to further support national policy.

ACCESSION NUMBER: ADA326624

http://handle.dtic.mil/100.2/ADA326624

Hamby, Janice M. ***Operational Protection of Information Technology Assets. A Commander's Guide to Risk Reduction***. Newport, RI: Naval War College, May 1997. 30p.

Abstract: Information technology (IT) is an essential part of any military action. The U.S. military increasingly relies on the force multiplier effect yielded by technological superiority and plans to conduct information warfare (IW) in future conflicts to minimize exposure and risk to forces. Despite the clear advantages that IT and IW can create for the combatant commander, their use is not risk free. Heavy dependence on IT yields a target rich environment for any adversary wishing to conduct his own IW campaign. Current developments in doctrine for IW do not adequately focus on the potential ramifications of IW and fail to highlight the criticality of the function of defensive IW (IW-D) and the operational protection of our extended IT infrastructure. Thoughtful, methodical approaches to minimize risk are

needed. This paper provides context for and proposes one such approach. Information technology (IT) is an essential part of any military action.

ACCESSION NUMBER: ADA328131

http://handle.dtic.mil/100.2/ADA328131

Hampton, Emanuel. ***Towards a National Strategy for Information Technology***. Carlisle Barracks, PA: Army War College, April 1999. 44p.

Abstract: In the 21st century, our national security and our continued economic prosperity will depend on how effectively we develop national strategies and policies to shape the development and use of information technology. Specifically, how should we develop current information technologies to meet future national needs. And how do we protect current information technology infrastructures from intellectual theft, sabotage, terrorism, information warfare, and natural disasters. To maintain our current technological advantage, the United States must remain the world leader in information technologies. To remain the world leader in information technology, the United States must maintain a viable national information technology strategy.

ACCESSION NUMBER: ADA363945

http://handle.dtic.mil/100.2/ADA363945

Harley, Jeffery A. ***Information, Technology, and the Center of Gravity***. Newport, RI: Naval War College, June 1996. 57p.

Abstract: The American 'way of war' emphasizes overwhelming force and advanced technology. Unfortunately, these factors may not be decisive in every type of conflict. Information and technology remain tools with limitations that are not fully recognized. Information systems are enhancing command and control as well as target acquisition. However, reliance on these tools limits the opportunity for operational innovation and obscures the use of planning tools. The center of gravity concept is limited by service perceptions and differing definitions. Common understanding of these tools of war would enhance their utility and help the United States fight better in the future.

ACCESSION NUMBER: ADA310922

http://handle.dtic.mil/100.2/ADA310922

Harley, Jeffery A. ***Role of Information Warfare: Truth and Myths***. Newport, RI: Naval War College, Joint Military Operations Department, 1996. 26p.

Abstract: The rapid growth in information technologies has generated three myths of information warfare: omniscience, obsolescence of armed forces, and information itself as a new center of gravity. Unfortunately, this obscures the true role of information technologies in better integrating information at all levels of warfare as well as creating an enhanced capability in synthesizing information with the better placement of ordnance on target. Information thus serves as a force multiplier and is best seen as a critical strength or vulnerability dependent upon the ability to exploit any information differential that may exist between opposing forces. At the same time, information technologies have had a pronounced effect upon the operational commander by enhancing and limiting mission planning, necessitating more complex information filtering, and through altering the commander's ability to execute a mission in a decentralized manner.

ACCESSION NUMBER: ADA307348

http://handle.dtic.mil/100.2/ADA307348

Hayes, J. L., et al. ***BM/C3 Information Technology Distributed Processing and Information Warfare***. Huntsville, AL: Army Space and Strategic Defense Command, 1997. 15p.

Abstract: The US Army Space and Strategic Defense Command (USASSDC) Advanced Technology Directorate (ATD) currently manages several research programs that have the potential to significantly advance the current state of the art in information technology for future Battle Management/Command,

Control, and Communication (BM/C3) systems. These programs address some of the challenges associated with full spectrum dominance in information warfare by providing new and innovative technologies for advanced distributed processing. The definition of information technology as it applies to BM/C3 is provided, as well as our vision for the future of distributed processing and its role in future BM/C3 systems. We propose that the realization of more effective BM/C3 systems utilizing megacomputer architectures to support the human in control will require continuing technological advances in high speed communications, architectural structures, automated decision support, modeling and simulation (MS), and parallel processing algorithms. The current research in optimistic computing, and photonic interprocessor routing and switching, and the applicability of this research to distributed BM/C3 is discussed. Finally, the future research plans including the application to the BMDO's development of a Virtual Distributed Hardware in the Loop (HWIL) Test Bed (VDHTB), are described.

ACCESSION NUMBER: ADA329064

http://handle.dtic.mil/100.2/ADA329064

Hosmer, C. and G. Gordon. ***Forensic Information Warfare Requirement Study***. Cortland, NY: Wetstone Technologies, 2002. 36p.

Abstract: The study presents an analysis of the state of the art in computer forensic technologies employed by the military, law enforcement, and business and industry sectors. Additionally, it charts the observed deficiencies in this area, by providing a research and development roadmap of consolidated requirements of all sectors of the economy which rely on the existence of a robust forensic toolset for accomplishing forensic computer investigations. An extensive survey of existing forensic tools was performed in order to develop a Forensic Information Warfare (FIW) Matrix that provides an in-depth look into the issues and the state-of-the-art technologies being used. The Computer Forensics matrix permitted the development and refinement of a FIW research and technology Road Map that integrates data from the FIW Matrix, with on-going university research, industry interests, and real forensic case data needs. The results provide a solid framework for determining the requirements for future R&D thrusts in computer forensic science.

ACCESSION NUMBER: ADA407355

http://handle.dtic.mil/100.2/ADA407355

Howard, J. D. “Security Incidents on the Internet, 1989--1995.” 15p. IN: ***INET98 - The Internet: Entering the Mainstream***, 8th Annual Networking Conference December 1995.

Abstract: This paper presents an analysis of trends in Internet security based on an investigation of 4,299 Internet security-related incidents reported to the CERT{reg_sign} Coordination Center (CERT{reg_sign}/CC) from 1989 through 1995. Prior to this research, knowledge of actual Internet security incidents was limited and primarily anecdotal. This research: (1) developed a taxonomy to classify Internet attacks and incidents, (2) organized, classified, and analyzed CERT{reg_sign}/CC incident records, (3) summarized the relative frequency of the use of tools and vulnerabilities, success in achieving access, and results of attacks, (4) estimated total Internet incident activity, (5) developed recommendations for Internet users and suppliers, and (6) developed recommendations for future research. With the exception of denial-of-service attacks, security incidents were found to be increasing at a rate less than Internet growth. Estimates showed that most, if not all, severe incidents were reported to the CERT{reg_sign}/CC, and that more than one out of three above average incidents (in terms of duration and number of sites) were reported. Estimates also indicated that a typical Internet site was involved in, at most, around one incident (of any kind) per year, and a typical Internet host in, at most, around one incident in 45 years. The probability of unauthorized privileged access was around an order of magnitude less likely. As a result, simple and reasonable security precautions should be sufficient for most Internet users.

REPORT NUMBER: SAND-98-8497C; CONF-98-0723

ACCESSION NUMBER: DE98052851

Hull, George B. ***Information Revolution and the Environment of Future Conflict***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1997. 87p.

Abstract: An information revolution is a fundamental and complete change in the way knowledge or intelligence is communicated and received. The heart of the revolution is the ability to communicate and receive information in ways never before possible. The consolidation of what became known as the Industrial Revolution, changed the way men worked and earned wealth, the way men governed themselves, the relations between nation-states, and the way men fought wars. The information revolution portends similar fundamental changes in society.

ACCESSION NUMBER: ADA331261

http://handle.dtic.mil/100.2/ADA331261

Hutcherson, Norman B. ***Command and Control Warfare. Putting Another Tool in the War-Fighter's Data Base***. Maxwell AFB, AL: Air University, Airpower Research Institute, September 1994. 78p.

Abstract: Command and control warfare (C2W) is the military strategy that implements information warfare (IW) on the battlefield. Its objective is to attack the command and control (C2) decision-making capabilities of an adversary while protecting friendly C2. C2W's focus is, sealing the eyes and ears of the enemy commander. It does this by disrupting and dominating the flow of information between the enemy's combat forces and their associated decision-making command elements. Ideally, through information dominance, friendly commanders will be able to work inside the enemy commander's decision-making cycle forcing him to be reactive and thus cede the initiative and advantage to friendly forces. In any conflict, from large scale transregional to small scale, localized counter-insurgency, a joint or coalition team drawn together from the capabilities of each service and orchestrated by the joint force or theater-level commander will execute the responses of the United States armed forces. Units should perform their specific roles in accordance with the doctrine and policies provided in joint publications. The training and execution of a unit's response and a commander's C2W actions should be based on doctrine, policies, and terminology provided in joint publications.

REPORT NUMBER: AU-ARI-941

ACCESSION NUMBER: ADA286005

http://handle.dtic.mil/100.2/ADA286005

Jensen, William J. ***Information Warfare's Missing Quarterback: The Case for a Joint Force Information Warfare Component Commander***. Newport, RI: Naval War College, Joint Military Operations Department, February 1998. 22p.

Abstract: The synergistic success of Information Warfare (IW) during Operation Desert Storm marked the birth of coordinated strategic and operational IW. Ironically, Desert Storm's 'textbook application' of IW has prevented subsequent joint IW operations from reaching their full potential and has hindered further IW organizational improvements. Challenging future joint operations are a diminishing military budget that is producing a smaller, interservice dependent force. Exacerbating the situation is the application of Desert Storm lessons learned, by potential adversaries, to their command and control systems. No longer can operational IW rely upon tactical redundancy to overcome ad hoc planning; the joint force commander (JFC) must get it right the first time. As a result of the Gulf War's robust application of IW, today's Commander in Chief (CINC) and joint force commander (JFC) can mistakenly think the current IW planning process promotes multiservice unity of effort. However, available methods to organize for the joint IW effort traditionally produce a powerless IW commander that plans and executes single dimension operations. To reap force multiplying effects that full spectrum IW can offer, the JFC must delegate sufficient coordinating authority and provide clear planning guidance to his IW commander. Unfortunately, current IW organization methods also fail to provide a reliable integrated planning process that allows seamless coordination across service boundaries. Implementation of a Joint Force Information Warfare Component Commander (JFIWCC) provides the IW commander with the authority to resolve current planning problems and execute multifaceted IW operations. The JFIWCC can compose the IW story' and

ensure its exacting performance--ultimately allowing the JFC to operate inside the adversary's decision cycle.

ACCESSION NUMBER: ADA349113

http://handle.dtic.mil/100.2/ADA349113

Jo, K. Y. and J. T. Dockery. "Virtual Network Representations of Information Warfare Battlespace." p. 457-461, IN: ***Military Communications Conference, 1998. MILCOM 98. Proceedings., IEEE***, v. 2. October 18-21, 1998. 1083p.

Abstract: Virtual network methodologies are applied to information warfare (IW) simulation in which objects and agents behave with special relationships. Decision makers operate in a virtual battlespace, which is in essence an information cyberspace in which IW attacks damage assessments, countermeasure efforts, and repairs are interrelated through virtual networks. The virtual network representation is used to model not only communications networks but also socio-technical networks with dynamic hyperactive characteristics. Different virtual network representations are realized to characterize various behaviors and to help generate associated performance measures. Communications network attacks will constitute a major source of IW activities that will be analyzed. Virtual networks are used to represent object behaviors with appropriate levels of abstraction depending on IW scenarios and problem domains.

Johnson, Robert E. ***Information Warfare: Impact on Command and Control Decision-Making***. Carlisle Barracks, PA: Army War College, April 1996. 31p.

Abstract: The military's senior leadership has openly acknowledged that in future wars we must win the information war to achieve decisive victory. This paper reviews decision--making when command and control (C2) systems are interrupted, contaminated, or destroyed. The United States is an information dominant society. For every technological advancement in the development of an offensive information-based system, our vulnerability to information warfare increases. Future conflicts will undoubtedly include threats to degrade our information systems. Are we training our leaders to respond in an environment where our information systems are corrupted, manipulated, or destroyed. As we prepare to 'Win the Information War,' our leaders must not allow predictable attacks on their information--based technology to force them toward unfavorable conflict resolution. 'Winning the Information War' must include contingency planning for disruptions in the flow of information.

ACCESSION NUMBER: ADA309107

http://handle.dtic.mil/100.2/ADA309107

Kadner, S., E. Turpen, and B. Rees. ***The Internet Information Infrastructure: Terrorist Tool or Architecture for Information Defense?*** Los Alamos National Laboratory, NM, December 1998. 17p.

Abstract: The Internet is a culmination of information age technologies and an agent of change. As with any infrastructure, dependency upon the so-called global information infrastructure creates vulnerabilities. Moreover, unlike physical infrastructures, the Internet is a multi-use technology. While information technologies, such as the Internet, can be utilized as a tool of terror, these same technologies can facilitate the implementation of solutions to mitigate the threat. In this vein, this paper analyzes the multifaceted nature of the Internet information infrastructure and argues that policymakers should concentrate on the solutions it provides rather than the vulnerabilities it creates. Minimizing risks and realizing possibilities in the information age will require institutional activities that translate, exploit and convert information technologies into positive solutions. What follows is a discussion of the Internet information infrastructure as it relates to increasing vulnerabilities and positive potential. The following four applications of the Internet will be addressed: as the infrastructure for information competence; as a terrorist tool; as the terrorist's target; and as an architecture for rapid response.

REPORT NUMBER: LA-UR--98-1348; CONF-98-0489

ACCESSION NUMBER: DE99000670

Kennedy, Kevin J., B. M. Lawlor and A. J. Nelson. ***Grand Strategy for Information Age National Security***. Carlisle Barracks, PA: Army War College, May 1996. 125p.

Abstract: Current national security strategy is obsolete. Based upon industrial age threats and defenses with limited information-age applicability, it fails to defend against structured information attacks threatening U.S. centers of gravity, and relies upon DoD as sole provider of national defense in the information dimension. U.S. technology dependence presents a strategic threat to the information systems that control key aspects of our national power. Future competitors may undermine our national will to fight by exploiting our reliance upon information systems, our present technological vulnerability. This threat would be most effective in situations where U.S. forces application is discretionary, and the desirability of employment is not obvious. The study proposes a strategic framework demonstrating the potential strategic effects of information weapons employment and conceptualizing both offensive and defensive information campaigns, highlighting shortfalls in present policies by suggesting accessibility of U.S. centers of gravity and limitations of protecting against employment of information weapons. It recommends that certain information systems, as strategic national security assets, require protection and demonstrates how strategic warfare's scope expands into the broader information dimension of conflict. Information assurance should be the theme for US defensive grand strategy, giving priority to the systems most essential to our national information infrastructure and systems that permit command and control and employment of military forces. A strategic plan for information assurance is offered.

ACCESSION NUMBER: ADA311158

http://handle.dtic.mil/100.2/ADA311158

Key, Olsen S. ***Impact of Information Warfare When Conducting Operational Deception***. Newport, RI: Naval War College, June 1996. 23p.

Abstract: U.S. military leaders placed a renewed emphasis on Operational Art in the late 1970s. The driving factor was the need to give operational commanders the tools necessary to better design campaigns to fill the gap between the strategic and tactical levels of war with a focus on translating national strategy into military objectives across the spectrum of conflict. The 'Revolution in Military Affairs' in the 1980s both enhanced and complicated this effort. Of particular difficulty was properly using expanding Information Warfare (IW) capabilities when planning and executing operational deception. Research reveals three areas where operational commanders may have to adjust their thinking in the operational design of the campaign plan: surprise, security, and boldness. Analysis of the use operational deception and IW in both the air and land campaigns in DESERT STORM reveals how CINCCENT blended these items into a successful operational deception plan. The lessons learned when the reviewing the planning and execution of the deception offer some insights into the use of operational deception with IW in future campaigns. U.S. planners and operational commanders cannot assume that the potential dominant battlefield awareness IW can provide will necessarily translate into successful deception operations.

ACCESSION NUMBER: ADA312053

http://handle.dtic.mil/100.2/ADA312053

Khalilzad, Zalmay M. and John P. White. ***Changing Role of Information in Warfare***. Santa Monica, CA: Rand Corporation, 1998. 462p.

Abstract: This effort to assess how the role of information in warfare is changing seeks to understand many of the remarkable developments under way in information and communications technology, and their potential effects on warfare. Indeed, this volume reveals several important lessons that can be gleaned from the very different and distinct perspectives contained in it: Information advances will affect more than just how we fight wars. The nature and purpose of war itself may change. How wars start, how they end, their length, and the nature of the participants may change as shifts in the relative power of states and nonstate entities occur. New technologies cut both ways in terms of their effects on national security. Together, the chapters make clear that advances create new vulnerabilities; new threats create new opportunities. We should resist the temptation to see the changes documented here either as wholly bad or wholly good. Rather, we need to understand that profound technological changes are inevitably two sided. The Department of Defense (DoD) has little control over the pace and direction of the

information revolution. Although in the past DoD played an important role in developing, refining, and implementing new information technologies, today the technological envelope is being pushed largely by the commercial sector.

REPORT NUMBER: RAND-MR-1016-AF
ACCESSION NUMBER: ADA364003
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
http://handle.dtic.mil/100.2/ADA364003

Killam, Timothy B. ***Weapons of Mass Disruption for the Operational Info-Warrior***. Newport, RI: Naval War College, February 1996. 24p.

Abstract: The technological advances of the information age have the potential for drastically altering contemporary ideas about power and its application. Future conflict and warfare have become inextricably intertwined with the information realm of cyberspace. Information Warfare (IW) is the logical extension of applying new and unconventional technologies to power projection and national defense. However, IW is not merely propaganda, command and control warfare (C2W), nor even simply a force multiplier in the operational toolbox. It is a way to control and attack the enemy's Observation, Orientation, Decision, and Action (OODA) loop. Instead of physically removing his 'center of gravity' C2 loop as in C2W and making him deaf, dumb, and blind, IW seeks to manipulate the OODA and the cyberspace in which it exists to make the enemy deaf, dumb, and blind to anything except that which we permit him to hear, say, or see. The Weapons of Mass Disruption (WMD) provide a new and unique capability to render the enemy's operational forces impotent by short circuiting the OODA loop and controlling the enemy's decisions and hence his courses of action. When combined with traditional military operations in a conventional war or OOTW, the effect can be quick, devastating, and decisive.

ACCESSION NUMBER: ADA307354
http://handle.dtic.mil/100.2/ADA307354

Kirk, David C. ***Artificial Intelligence Applications to Information Warfare***. Carlisle Barracks, PA: Army War College, March 1996. 35p.

Abstract: In the coming years, a critical element of combat will likely be waged in the information infrastructure. Current strategic concepts do not compensate for the vulnerability of our ever-increasing information-based society. In this research project, artificial intelligence technology (specifically, intelligent agents) was explored. Intelligent agents were found to have characteristics that could help execute an information war. Although there still is work to be done, intelligent agents may someday manage the information flow, be the core technology in network firewalls, and contribute to overall network security through continuous Red Team vulnerability assessments.

ACCESSION NUMBER: ADA309400
http://handle.dtic.mil/100.2/ADA309400

Klinefelter, Stephen. ***National Security Strategy and Information Warfare***. Carlisle Barracks, PA: Army War College, April 1997. 35p.

Abstract: This paper examines how the National Security Strategy (NSS) and its new subcomponent, the National Security Science and Technology Strategy (NSSTS) address Information Warfare. The Executive Branch has put the Department of Defense (DoD) on the front lines of the national effort to define and build a National Information Infrastructure (NII). The Defense information Infrastructure (DII) is described in its relationship to the NII. Two information systems of the DoD are then examined. They are: Electronic Commerce/Electronic Data interchange (EC/EDI) and the Defense Message System (DMS). They are described nontechnically to press home three points. First, Information is a national strategic asset and that using it and protecting it should be national priorities. Second, the world and the United States are becoming extremely interconnected and interdependent during this information Age. This represents a new dimension of warfare and national security across all levels of conflict and all locations of the battlespace. The NSS and the NSSTS should explicitly recognize Information Warfare, probably

under a different diplomatically acceptable name. Third, the Administration recognizes these trends and has accounted for them in the NSS even if not explicitly recognized.

ACCESSION NUMBER: ADA326621

http://handle.dtic.mil/100.2/ADA326621

Kluepfel, H. "Countering Non-Lethal Information Warfare: Lessons Learned on Foiling the Information Superhighwayman of the North American Public Switched Telephone Network." p. 474-479, IN: ***Security Technology, 1995***. Proceedings. Institute of Electrical and Electronics Engineers 29th Annual 1995 International Carnahan Conference, 18-20 October 1995. 512p.

Abstract: The United States relies for its very existence-economically, socially, and politically-on an extraordinary sophisticated and intricate set of long distance networks for energy distribution, communication, and transportation. In addition to their serious vulnerabilities to accidents and nature, these networks present a tempting target to terrorists and to any antagonist contemplating an international move contrary to US interests. While warnings such as the one cited above predicted potentially catastrophic consequences, the fragility of today's global networks of computer based systems, used to business process reengineer America's industrial and military infrastructure into lanes on the information superhighway, together with concerns over information warfare, are taking front burner attention on the agenda's of military and civilian agencies within the United States. The paper describes and helps to further set the stage for the establishment and realization of a defensive information warfare security baseline architecture for the NII information superhighway and its global partners and components throughout their lifecycle, from research and development to deployment and beyond.

Koehler, Stephen T. ***Operational Level of War: Radical Change Needed to Support the American RMA***. Newport, RI: Naval War College, February 1999. 27p.

Abstract: Information technology continues to grow at an enormous pace all over the world, increasing the speed of information exchange and subsequent availability of knowledge. The industrial age has given way to the information age, and the truth of the adage, knowledge is power will yield a vast array of wielders that will require strong leadership to contain. For operational commanders to maintain an advantage over other emerging information savvy opponents, they must fundamentally alter the way operations are conducted and must do so now. The fundamental factors of time, space and force will still apply in a futuristic world where arguably instantaneous information will allow a completely clear battlefield. Regardless of how it is done the operational commander must still dictate all three. The lessons learned in the past will provide future foes the necessary tools to exploit an American weakness; the speed of maneuver has not kept pace with the speed of strike, let alone the speed of information. The technology is presently here to alter the way that the United States fights in a CONUS to Objective Maneuver that increases the speed of maneuver to one that matches both the speed of strike and the speed of interaction in a globally connected society. The U.S. military must start changing its concepts to drive technology to meet them, thereby dictating a huge space with a mandated smaller force and shorter time. To not adjust now will leave the United States with a weakness that they helped foster.

ACCESSION NUMBER: ADA363061

http://handle.dtic.mil/100.2/ADA363061

Komar, David M. ***Information-Based Warfare: A Third Wave Perspective***. Maxwell AFB, AL: Air University, Air War College, May 1995. 42p.

Abstract: The information revolution provided the technology to process vast amounts of data and make it accessible instantaneously and simultaneously to anyone anywhere in the world. The Tofflers proposed a model which depicts a trisected world with societies categorized by how they make wealth. The most advanced wave, the Third Wave, creates wealth through knowledge. Consistent with the Tofflers' model, economies of Third Wave societies are becoming more and more dependent upon knowledge. The effects of the information revolution on the global economy have made the wealthy nations more vulnerable to information-based warfare against the economic instruments. If the Tofflers' model

accurately depicts the wealth generation methods of the Third-Wave, then the most likely future war-form is information-based warfare against the economic instruments. Third Wave societies are ill-prepared to defend against this new war-form. The advanced nations must recognize their vulnerabilities and develop the policies and means to protect themselves against these new threats.

ACCESSION NUMBER: ADA328862

https://research.maxwell.af.mil/viewabstract.aspx?id=1637

http://handle.dtic.mil/100.2/ADA328862

Kurdys, Martin P. ***Information Warfare (IW) Command and Control Warfare (C2W) for the Naval Expeditionary Task Force Commander***. Newport, RI: Naval War College, April 1996. 27p.

Abstract: The bottom line to a Commander of a Naval Expeditionary Force is how Information Warfare (IW) and Command and Control Warfare (C2W) can increase the operational effectiveness of the force responding to a contingency. To get there, one must examine the national strategic role of IW, the traditional role of the Naval Expeditionary Force, and the operational role of C2W. From these, an operational level approach to IW/C2W can be developed that is both consistent with strategy and doctrine and useful to the Commander of a Naval Expeditionary Force.

ACCESSION NUMBER: ADA312051

http://handle.dtic.mil/100.2/ADA312051

Lankhorst, Debra A. ***Using Expert Systems to Conduct Vulnerability Assessments***. Monterey, CA: Naval Postgraduate School, September 1996. 111p.

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

ACCESSION NUMBER: ADA319367

http://handle.dtic.mil/100.2/ADA319367

Leney, Derek J. ***Improving Information Warfare Targeting: An IW Fires System.*** Newport, RI: Naval War College, Joint Military Operations Department, February 1995. 30p.

Abstract: Information Operations (IO) has grown in importance during recent conflicts. Yet some aspects of IO coordination and integration have fallen short of expectations. This has led to a desire by many in the IO community to better manage Information Warfare "fires" using the Joint Targeting Cycle as a rational process for their execution. However, current doctrine and joint organizations do not adequately provide for control of these fires. This paper addresses the conceptual challenges of Information Warfare (IW) targeting, including the differences between attacking "will" and attacking "capability." Recent lessons learned in Iraq and Kosovo highlight additional IO problems within the Joint Targeting Cycle. An IW Fires System is proposed to address these shortcomings, providing a formalized and connected organization for IW targeting and fire support.

ACCESSION NUMBER: ADA465003

http://handle.dtic.mil/100.2/ADA465003

Luiijf, H. A. M. ***Survey of Information Warfare, Information Operations and Information Assurance.*** The Hague, Netherlands: Fysisch en Elektronisch Laboratory, 1999. 92p.

Abstract: Research survey on the phenomena Information Warfare, Information Operations (Info Ops) and Information Assurance. History, development, definitions and developments in various countries around the globe. Appendix with list of abbreviations of terms in these fields.

ACCESSION NUMBER: ADA367670

http://handle.dtic.mil/100.2/ADA367670

Littleton, Matthew J. ***Information Age Terrorism: Toward Cyberterror***. Monterey, CA: Naval Postgraduate School, December 1995. 150p.

Abstract: The growing ubiquity of computers and their associated networks is propelling the world into the information age. Computers may revolutionize terrorism in the same manner that they have revolutionized everyday life. Terrorism in the information age will consist of conventional terrorism, in which classic weapons (explosives, guns, etc.) will be used to destroy property and kill victims in the physical world; technoterrorism, in which classic weapons will be used to destroy infrastructure targets and cause a disruption in cyberspace; and cyberterrorism, where new weapons (malicious software, electromagnetic and microwave weapons) will operate to destroy data in cyberspace to cause a disruption in the physical world. The advent of cyberterrorism may force a shift in the definition of terrorism to include both disruption and violence in cyberspace in the same manner as physical destruction and violence. Through the use of new technology, terrorist groups may have fewer members, yet still have a global reach. The increasing power of computers may lower the threshold of state sponsorship to a point where poor states can become sponsors and rich states are no longer necessary for terrorist groups to carry out complex attacks. This thesis explores the shift toward information warfare across the conflict spectrum and its implications for terrorism. By examining the similarities and differences with past conventional terrorism, policymakers will be able to place information age terrorism into a known framework and begin to address the problem.

ACCESSION NUMBER: ADA306243

http://handle.dtic.mil/100.2/ADA306243

Litton, Leonard G. ***Information-Based RMA and the Principles of War***. Newport, RI: Naval War College, February 1999. 25p.

Abstract: The U.S. military is currently experiencing a Revolution in Military Affairs (RMA) which has the potential to increase its combat capability orders of magnitude over any potential adversary. The essence of this revolutionary affair is that the character and conduct of warfare is undergoing a significant change driven primarily by the ability to acquire, collect, disseminate, and employ information in a very rapid manner. Conversely, there are many reason to believe that warfare is more evolutionary than revolutionary. There is a body of thought that suggests that there has always been in existence certain principles of war that are immutable, timeless, and independent of place or situation. If the information based RMA really has the potential to deliver on its promises, we must begin to embrace it by reexamining the underlying elements of our doctrine, the principles of war, and insure they lay the proper foundation for the military of the 21st century. We should challenge the current paradigms we hold and begin to think of these principles in new ways, some being radical departures from the old school solution. We must choose our words and definitions in our publications carefully, for they serve to convey to our soldiers what we hold to be true about the ways in which we wage war.

ACCESSION NUMBER: ADA363157

http://handle.dtic.mil/100.2/ADA363157

Lofaro, A. “The Cultural Factor in Information Warfare.” p. 11-17, IN: ***Technology and Society, 1998. ISTAS 98. Wiring the World: The Impact of Information Technology on Society***, Proceedings of the 1998 International Symposium, 12-13 June 1998. 176p.

Abstract: In its most general meaning, information warfare is based on disrupting, faking or limiting access to information by whatever opponent you have. Usually, information warfare analyses are centered on the technical skills needed, on the specific instruments used and how to use them, and even (mainly in threat analysis) on the motivations that could push someone to use old, direct methods or more sophisticated kind of attacks. Thanks to its effects on how somebody (and even a social group) reacts to information, an important factor in the possibility, effectiveness and likelihood of an information warfare attack is the cultural framework in which the attack is done, or (wherever different) the mutual interactions between the cultural frameworks of the attacker and the attacked opponent. In this paper, I look at some example of different reactions to information taken from various cultural contexts and from various fields (like advertising, software localisation and international working environments) in which the problem has already been studied, and I try to show how this can affect information warfare, making this a variable which must be accounted for every time in order to make an effective analysis.

Luoma, William M. ***Netwar: The Other Side of Information Warfare***. Newport, RI: Naval War College, Department of Operations, February 1994. 40p.

Abstract: The JCS' recognition of Information Warfare as an important area of concern has resulted in the promulgation of policy for development of the Command and Control Warfare (C2W) concept. However, while intended to be employed across the spectrum of conflict, C2W is oriented more toward military objectives and lacks completeness as a strategy when viewed against the plethora of future national security threats. In many of these instances, use of military force may not always be an effective or credible expression of national power for the theater CINC when executing his Joint Strategic Capabilities Plan responsibilities. The network or Netwar concept complements C2W as an Information Warfare strategy which can provide a vehicle for action in scenarios where application of military force is not appropriate and/or during operations other than war. To be effective, the Netwar strategy requires coordination of all elements of national power to counter and neutralize the power of network adversaries. Application of Netwar in support of non-military Flexible Deterrent Options provides a framework for analysis.

ACCESSION NUMBER: ADA27958

http://handle.dtic.mil/100.2/ADA279585

Marr, Patrick M. ***Information Warfare and the Operational Art***. Newport, RI: Naval War College, February 1996. 24p.

Abstract: Command and Control Warfare (C2W), the military strategy for implementing Information Warfare (IW), is self-limiting by definition. Taken individually, the components of C2W - OPSEC, PSYOP, EW, military deception and physical destruction - - are not indicative of the information revolution. The continued effort to expand the military strategy of IW beyond the current bounds of C2W may be indicative of a technology-strategy mismatch or disconnect.

ACCESSION NUMBER: ADA307441

http://handle.dtic.mil/100.2/ADA307441

McCauley-Bell, P. and R. Freeman. “Quantification of Belief and Knowledge Systems in Information Warfare.” p. 1597-1585, IN: ***Fuzzy Systems, 1996, Proceedings of the Fifth IEEE International Conference, 8-11, September 1996***. Vol. 3

Abstract: This research presents an application of fuzzy set theory (FST) to the management of uncertainty in information warfare. Emphasis is placed on evidence accrual in the context of uncertain and/or incomplete performance. This analysis considers the observe-orient-decide-act (OODA) loop and the human responses in these four stages. The methodology proposes the analysis of evidence accrual by categorizing responses in the OODA loop as a result of knowledge systems and belief systems. A fuzzy approach is use to measure each of these systems. This approach considers distributed task

accomplishment in information warfare such as surveillance, ground or air based command, control, communication, computers, intelligence sensors, and reconnaissance (C4ISR), and F-15E attack, systems.

McCauley-Bell, P. and R. Freeman. "Uncertainty Management in Information Warfare.: p. 1942-1947, IN: ***Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation, 1997 IEEE International Conference,*** 12-15 October, 1997. Vol. 2.

Abstract: This paper investigates the application of fuzzy uncertainty management to information warfare simulation (SimIW). Information warfare (IW) is manifested in uncertainty; no resolved or conclusive definition currently exists. From the creation of false signals to alteration of network performance, uncertainty is rooted in this type of combat. A model for defining the types of cognitive systems that perceive information is presented as well as an explanation of the types of uncertainty associated with information. The measurement of uncertainty associated with this project is managed using fuzzy logic. Fuzzy logic manages different types of uncertainty and provides a linguistic modeling capability that more closely match that of the human communications capability. The chosen application was to develop an example of a fuzzy generic intelligent agent where this agent is an active participant in IW. The project provides a model of how an agent will characterize and measure associated uncertainty.

McCollum, William W. ***Role of the Intelligence Community in Preparing to Win the Information War***. Carlisle Barracks, PA: Army War College, April 1997. 25p.

Abstract: Increasing reliance on information-based technology is not unique to the United States, but growing awareness of the vulnerabilities created by this reliance has focused attention on protecting our information and information systems, while the potential value of offensive information operations, particularly in peacetime, has been less fully explored. This paper examines the relationship between defensive and offensive information warfare, looks at the status of governing policies and doctrine, discusses the vital role of intelligence in winning the defensive and offensive information war, and makes recommendations regarding organizing the intelligence community to support the successful prosecution of the offensive information war.

ACCESSION NUMBER: ADA326646

http://handle.dtic.mil/100.2/ADA326646

McKethan, Colton. ***U.S. C4I and Logistics Vulnerabilities to Offensive Information Warfare***. Newport, RI: Naval War College, June 1997. 31p.

Abstract: The information revolution fostered by the microchip has made it possible for military commanders to receive information in unequaled quantity and quality. U.S. commanders have a broad range of opportunities resulting from digitized technologies that enhance of military equipment performance and the application of force. These information advances represent force enablers providing synergistic advantage to operational command and control (C2), intelligence, and logistic functions. However, there is a down side, in that the computers and microchips have vulnerabilities that must be addressed to retain operational force advantage. Information warfare is central to the way the nation plans to fight in the future, and information systems now connect U.S. military forces on a worldwide basis. Despite the enhancements that connectivity brings, with integration of global communications, state and non-state actors are provided new ways to access and undermine the C2, intelligence, and logistics function via computer and communication networks. This new area of vulnerability extends from the strategic, through the operational, down the tactical levels of warfare. State and non-state actors have means of attacking core military centers of gravity and critical strengths without resorting to conventional attack or deception. Today, joint commanders and civilian leaders must seriously consider the ramifications of unwanted intrusion into the national and defense information infrastructures. As U.S. forces become increasingly dependent on information to leverage battlespace awareness the need to protect information systems will increase. Backup capability must be designed into the information infrastructure to preclude erosion of force application capability.

ACCESSION NUMBER: ADA328226
http://handle.dtic.mil/100.2/ADA328226

McLendon, James W. ***Information Warfare: Impact and Concerns***. Maxwell AFB, AL: Air University, Air War College, April 94. 42p.

Abstract: Information has always been a critical factor in war. Clausewitz said 'imperfect knowledge of the situation... can bring military action to a standstill.' Sun Tzu indicated information is inherent in warfighting. Information warfare embodies the impact of information on military operations. The computer age gives us the capability to absorb, evaluate, use and transmit and exchange large volumes of information at high speeds to multiple recipients simultaneously. Multiple sources of data can be correlated faster than ever. Thus, the value of information to the warfighter has been magnified to a new level. Churchill used information warfare when he used the ENIGMA machine to read German codes during World War II. He also used information warfare through his elaborate network emanating from the London Controlling Section, for its time a very complex intelligence and deception operation.

ACCESSION NUMBER: ADA328933
https://research.maxwell.af.mil/viewabstract.aspx?id=1648
http://handle.dtic.mil/100.2/ADA328933

Mengxiong, Chang. ***Prospects For Weapons, Troops, and Battlefields in the Information Age***. Wright-Patterson AFB, OH: National Air Intelligence Center, February 1996. 37p. Translation of unknown Chinese source, np nd.

Abstract: This is a high-level soft scientific research report in predicting future developments in military trends. In the fundamental viewpoint, weapons and troops are currently on the eve of great technical innovation. Weapons and troops in the 21st century are the 'informationized' weapons and troops. Their concrete realization constitutes 12 aspects: informationized ammunition, informationized soldiers, informationized combat platform, defense information system (C3I), informationized weapon system, informationized battlefield, information warfare, information intimidation, combat command system with combination of high centralization and high automation, as well as smooth transition from virtual weapons and virtual battlefields toward real weapons and real battlefield. Intensity is the matrix indicator of troops in the 21st century; troops will be the highest cultural and technical component in the society, as the informationized weapons still require other technical supports. In the last part of the paper, a 28-character methodology is presented by the author in studying weapons and troops of the 21st century: based on major technical progress, new conceptual weapon systems are set forth, new types of combat are initiated.

ACCESSION NUMBER: ADA306614
http://handle.dtic.mil/100.2/ADA306614

Minehart, Robert F., Jr. ***Information Warfare: The Organizational Dimension***. Carlisle Barracks, PA: Army War College, February 1996. 27p.

Abstract: Since the December 1992 publication of the Department of Defense (DOD) classified directive on Information Warfare (IW) considerable effort has been expended examining this issue. Despite this attention, a clear vision for the implementation of IW within DOD and the U.S. Government as a whole has yet to emerge. Three pillars are essential to achieving a viable IW strategy and supporting architecture: policy doctrine, organization training and requirements/technology. Much has been written, discussed, and even debated on the need for overarching national policy in this area, as well as the multitude of capabilities and vulnerabilities stemming from our increased reliance on advanced technology. A similar focus on the organizational component of IW has not occurred. The study specifically addresses the role of organizations as a key component of IW. Both the progresses achieved to date within DOD and the significant challenges remaining to be overcome at the interagency level are examined. Specific recommendations are provided on how better to organize the IW effort.

ACCESSION NUMBER: ADA309782

http://handle.dtic.mil/100.2/ADA309782

Moore, Joe W. ***Information Warfare, Cyber-Terrorism and Community Values.*** Wright-Patterson AFB, OH: Air Force Institute of Technology, 2002. 155p.

Abstract: Information Warfare involves the attack and defense of information and information systems, both in time of armed conflict and in operations short of war. While information technology provides the promise of a new class of less lethal military instruments, it also presents vulnerabilities occasioned by widespread dependence on an increasingly complex and interconnected global information infrastructure. These vulnerabilities, when exploited by those who would target civilians in order to inspire widespread fear in hopes of accomplishing a political agenda, can be understood as cyberterrorism. As information warfare techniques evolve, those employing them should look to several relevant sources for normative guidance. Relevant, internationally shared values can be found in international custom, the U.N. Charter, treaties dealing with the subject of "cybercrime," those governing the communication media likely to be utilized by information warriors, UNGA Resolutions and those treaties and customary norms that make up the Law of Armed Conflict.

ACCESSION NUMBER: ADA410710

http://handle.dtic.mil/100.2/ADA410710

Mullis, William S. ***Using the Acquisition Process to Reduce the Vulnerability of Future Systems to Information Warfare.*** Monterey, CA: Naval Postgraduate School, March 1997. 78p.

Abstract: Information warfare (IW) is a growing concern for the United States Army. The sophisticated, high-technology modern weapons systems upon which the U.S. Army heavily relies are increasing vulnerable to IW weapons and tactics. The acquisition process plays a major role in reducing defense systems IW vulnerability. This research identifies the primary IW threats to systems during the acquisition lifecycle and what factors in the acquisition environment contribute to IW vulnerability. This research also suggests a technique for integrating IW countermeasures into the defense systems acquisition process. A primary finding of this research is that while a Program Management Office (PMO) can institute a myriad of useful countermeasures, influencing the prime contractor to establish a secure development environment is the most important action it can take in reducing the vulnerability of future systems to IW.

ACCESSION NUMBER: ADA331209

http://handle.dtic.mil/100.2/ADA331209

Nault, Mark. ***General! They've Captured Our Hard Drive!*** Carlisle Barracks, PA: Army War College Strategic Studies Institute, November 1997. 35p.

Abstract: Joint Vision 2010 (JV 2010), an overview document describing the strategic vision of the Chairman of the Joint Chiefs of Staff (CJCS), was released in early 1997 and revealed a new joint armed forces battlespace concept called Full Spectrum Dominance (FULL SPECTRUM DOMINACE). Information Operations (IO), which includes both Information Warfare (IW) and Command and Control (C2) doctrine, is the backbone of this emerging JV 2010 FULL SPECTRUM Dominance concept. Are there any significant strategic level IO concerns, for our military leaders who practice the strategic art in today's and tomorrow's joint armed forces, which ultimately delay or degrade the capabilities detailed in the new JV 2010. This author believes that the answer to this thesis question is a resounding YES This Strategic Research Project (SRP) briefly reviews several basic, but recently updated, IO definitions, and describes the role that IO plays in the cyber missions depicted in the new JV 2010 and other related documents, such as the President's National Security Strategy (NSS), the Quadrennial Defense Review (QDR), the CJCS's National Military Strategy (NMS), as well as individual service concept documents. Furthermore, this SRP brings to light several key issues, which have the potential to negatively impact the total package, previously referred to as Full Spectrum Dominance. Several recommendations are also included, as food for thought for those who are now, or soon will be working hard in the strategic joint arena.

ACCESSION NUMBER: ADA342284

http://handle.dtic.mil/100.2/ADA342284

Nelson, Ronald J. ***Strategic Information Warfare National Information Infrastructure and the Defense of the Nation***. Carlisle Barracks, PA: Army War College, March 1998. 54p.

Abstract: The national information infrastructure is critical to broad segments of U.S. society, from business and government to the military. Reliance on the information infrastructure to streamline business processes is saving resources and increasing short-term competitiveness. However the competitive global environment that is driving business to streamline allows little margin for disruption of business information flow. Disruptions of business processes that rely on the information revolution could lead to offshore migration or outright concession of segments of U.S. industry to foreign competitors. Legal ambiguities abound in almost every aspect of infrastructure assurance. Significant strategic thinking is required to resolve ambiguities in the domestic and international information environments that affect infrastructure assurance and deterrence through offensive or defensive use of information warfare. Cyberspace is not geographically bounded; the legal landscape must expand beyond physical boundaries and material property rights if infrastructure assurance is to be achieved. Since security measures have not kept pace with the explosion in technology associated with the information revolution, the purpose of this paper is to determine if the information infrastructure is at risk, and to conclude what coherent steps must be taken to both increase awareness of the threat and protect the U.S. information infrastructure. Moreover, second order effects of the information revolution need to be studied to insure that long term competitiveness of U.S. business is not placed at risk by external information operations.

ACCESSION NUMBER: ADA341299

http://handle.dtic.mil/100.2/ADA341299

Newman, Herb W. ***Digital Data Warfare Tools: Should CINCs Have Control***. Carlisle Barracks, PA: Army War College, March 1999. 51p.

Abstract: The meteoric explosion of information-age technologies led by the ongoing rapid evolution of cyberspace and microcomputers has brought about a revolution in Military Affairs. A new form of Information Operations (IO) warfare, Digital Data Warfare, portends enormous ramifications for the national security of the United States, its allies, and potential coalition partners. Joint Pub 3-13 provides doctrine for the execution of IO in joint operations. It discusses integration and synchronization of offensive and defensive IO in the planning and execution of combatant commanders' plans and operations to support the strategic, operational, and tactical levels of war. What Joint Pub 3-13 does not do is state that combatant commanders should have control of Digital Data Warfare tools. This paper examines and answers important strategic questions concerning combatant commander's control and authority to employ offensive Digital Data Warfare tools. The guideposts of this study provide a primer for understanding control and employment of Digital Data Warfare.

ACCESSION NUMBER: ADA364586

http://handle.dtic.mil/100.2/ADA364586

Nowowiejski, Dean A. ***Concepts of Information Warfare in Practice: General George S. Patton and the Third Army Information Service, August-December, 1944***. Fort Leavenworth, KS: Army Command and General Staff College, March 1995. 57p.

Abstract: This monograph looks for historical examples of information warfare in order to gain insight into its current practice. It first describes key elements of the concept of information operations, particularly as they relate to battle command. It then explores how George S. Patton and his Third Army Information Service demonstrated those ideas, and how their example offers direction for current developments in information warfare. Key sources used in research included emerging doctrinal literature on information warfare, biographical information on the professional development and command qualities of Patton, and after action reports of the Third Army and 6th Cavalry Group, the unit that constituted the Army Information Service. This monograph found that Patton aggressively sought information advantage as a battle commander, and that he demonstrated the key qualities of vision and intuition. The Third Army

Information Service developed a relevant common picture of the battlefield by the expanding the instrument of directed liaison. What needs emphasis in current concept of information warfare is the improving the ability of commanders and staffs to process information. We must reemphasize the human dimensions of information operations through refined professional development.

ACCESSION NUMBER: ADA301155

http://handle.dtic.mil/100.2/ADA301155

Okello, Fredrick, et al. ***Information Warfare: Planning the Campaign***. Maxwell AFB, AL: Air University, Air Command and Staff College, April 1996. 78p.

Abstract: Information warfare is a nebulous concept, but widely cited as a keystone in any future campaign. Even though information warfare has been used for centuries, current doctrine, policies, and guidance provide little help for the warrior to understand first, what information warfare is, and secondly, how to do it. 'Information Warfare: Planning The Campaign' provides a logical approach for the information warrior to employ in planning for this aspect of warfare. This paper addresses the: (1) Current state of information warfare policy and doctrine, (2) Modeling of a system to identify its critical nodes and links, (3) Modeling of a Joint Forces Air Component Commander (JFACC) to serve as an example, (4) Examples of current and potential offensive and defensive information warfare tools used in information encounters, and finally, and (5) A step-by-step approach to information warfare campaign planning. Analysis of information and its flow is a daunting undertaking in all but the most simple of organizations. To remedy this, one can view the organization as a system and employ a model which will help illustrate information flows. It is reasonable to employ the same model for this purpose as is used by system engineers who create information systems. This paper describes such a model, the Operational Architectures Model, which employs the Integrated Computer Aided Manufacturing (ICAM) Definition Methods or IDEF for short, to identify the flow of information in a system. Internal to the Operational Architectures Model are five modeling perspectives: functional, physical, static, informational, and dynamic.

ACCESSION NUMBER: ADA331946

http://handle.dtic.mil/100.2/ADA331946

Olbrys, Elizabeth B. ***Information Culture in DoD: Preparing for the Third Wave***. Washington, DC: Industrial College of the Armed Forces, April 1994. 36p.

Abstract: Is the Department of Defense prepared to receive, process and share information according to the model of the information superhighway. If we are, how will the Department of Defense be changed by adopting the new information-sharing model over our current information-control. As our war-fighting model evolves from attrition warfare to information warfare (Alvin Toffler's third wave warfare), swift access to current, reliable information will become our most basic requirement. If we are to maximize future readiness and achieve the cost reductions promised from the information superhighway, the Department of Defense must make major cultural changes. We must achieve enterprise integration, embrace the culture of process improvement, and accept a radical reorganization in order to realize information superiority--and therefore military superiority--on the battlefield.

ACCESSION NUMBER: ADA288500

http://handle.dtic.mil/100.2/ADA288500

Panda, Brajendra and Thomas Wiggins. ***Damage Assessment and Recovery from Information Warfare Attacks.*** Fargo, ND: North Dakota State University, Department of Computer Science and Operations, 2002. 6p.

Abstract: Sensors at different Air Force operation sites collect information on various system parameters and send to the Air Force Computer Emergency Response Team (AFCERT) for analysis. Due to the massive amount and complex nature of data involved, this process, however, is inefficient and time consuming. It is rather desirable that each site pre-processes the data before transmitting to the AFCERT. For efficient processing of data at both local and global sites, development of a suitable format for storing data locally, and determining characteristics desired at the global site for the fusion of data

obtained from different sites are important. In this research, the following issues have been addressed: 1) reduction of collected information for the diagnosis of attack, 2) efficient analysis of resultant data, 3) fast and accurate damage assessment, and 4) real-time recovery of the system.
ACCESSION NUMBER: ADA406469
http://handle.dtic.mil/100.2/ADA406469

Payne, Allan D. ***Impact of Computer Network Attacks on Infrastructure Centers of Gravity***. Carlisle Barracks, PA: Army War College, April 1999. 29p.
Abstract: Computer Network Attack is a significant asymmetric threat to the United States and its military. Motives vary, but the threat from CNA is real; US infrastructure targets are vulnerable; those that directly affect the ability of the US military to conduct its missions are evident Innovation in CNA is unrestrained, and privacy rights of the US citizenry conflict directly with US government efforts to take active measures to help defend against CNA. CNA today could be economically damaging to the computer and network dependent society that the United States has become. The challenge is to define the problem separately from every other consideration and challenge that the military faces in the Information Age including the broader mission areas of Information Operations and Information Warfare.
ACCESSION NUMBER: ADA364072
http://handle.dtic.mil/100.2/ADA364072

Pears, Andrew H. ***Planning for the Information Campaign***. Masters thesis. Wright-Patterson AFB, OH: Air Force Institute of Technology, May 1996. 69p.
Abstract: Desert Storm demonstrated the importance of dominating the information realm during a conflict. Information warfare is the means through which our forces can maintain information dominance on future battlefields. Air Force doctrine is currently being modified to include three new roles and missions related specifically to information warfare. Plans for future conflicts should include these new roles and missions. Campaign plans serve as the unifying focus for our conduct of warfare. This study examines the various aspects of campaign planning and information warfare. This research provides future planners eight specific information campaign planning recommendations. It is recommended that the information campaign plan support the joint effort, follow the fundamentals of campaign plans (JCS Pub 5-0), and accomplish information warfare objectives. Furthermore, information campaign planners should examine communications network survivability, friendly and enemy centers of gravity, satellite systems capabilities and vulnerabilities, the possible effects of the media and specific user requirements.
ACCESSION NUMBER: ADA309717
http://handle.dtic.mil/100.2/ADA309717

Peifer, Kenneth V. ***Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy***. Wright-Patterson AFB, OH: Air Force Institute of Technology, December 1997. 178p.
Abstract: This study focused on determining if unclassified current and pending Air Force information warfare and information operations doctrine and policy is moving in the direction it should in terms of being complete, consistent and cohesive based on what has been mandated and studied about information warfare. A model of unclassified current and pending Air Force information warfare and information operations doctrine and policy was examined through criterion-based congruence analysis to make this determination. Investigative questions were developed in reference to the current state of unclassified Air Force information warfare and information operations doctrine and policy. Secondary data analysis was conducted along two paths. The hierarchical path included an examination of unclassified information warfare and information operations doctrine, policy and regulatory guidance. The academic path included an examination of studies and commentary on information warfare and information operations focusing on doctrine and policy. A model of unclassified current and pending Air Force information warfare and information operations doctrine and policy was developed. Then the model was analyzed for congruence in terms of completeness, consistency, and cohesiveness using the hierarchical

and academic secondary data analysis as a diagnostic tool. The model was found to be partially incongruent in all three areas.

REPORT NUMBER: AFITGIRLAS97D10
ACCESSION NUMBER: ADA340379
https://research.maxwell.af.mil/viewabstract.aspx?id=1208
http://handle.dtic.mil/100.2/ADA340379

Perusich, K. "Information Warfare: Radar in World War II as an Historical Example." p. 92-99, IN: ***Technology and Society, 1997. 'Technology and Society at a Time of Sweeping Change'. Proceedings***, 1997 International Symposium, 20-21 June 1997. 328p.

Abstract: Emerging technologies have increased the capability to acquire and use data as a weapon in warfare. Although aggregated under a common term, information warfare actually represents a variety of different ways with different actors in different environments that information can be used as part of an arsenal. One important form of information warfare is decision making (or OODA-loop) warfare, in which a defender or attacker uses information acquisition or processing technology to complete their decision making cycle quicker than an opponent can to maintain the initiative in the battle. Such a type of information warfare was used during the Battle of Britain in World War 2. Radar was an enabling technology that gave Great Britain an edge in the decision making process that contributed to England's ultimate victory in the battle.

Phillips, Gary E. ***Information Operations - A New Tool for Peacekeeping***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1997. 92p.

Abstract: This monograph discusses the application of information operations to improve the efficiency and effectiveness of peace missions ranging from peacekeeping to peace imposition. Using a variety of models and an examination of the components of information operations this monograph demonstrates the applicability of these operations to peace missions. Examples from recent history provide a backdrop for evaluating previous applications and investigating other potential uses of information operations to support peace missions. Based on the validation of applicability the possible increase in effectiveness and efficiency are postulated and potential resource savings evaluated. The monograph first examines the status of international relations as a result of the demise of the Soviet Union and the rise of information technology. The impact of these two earthshaking events have forever changed the face the world. As the nations of the world seek a new geometry of relationships without the Soviet Union the level of violence continues to rise. Without the unifying ideologies of the Cold War, many nations are seeking identity through ethnicity. This factor in conjunction with a freedom to act completely in promotion of national interests without the specter of a global nuclear war has led to a very unstable world. At the same time that United Nations pleads for resources to enforce peace on the new world disorder, nations are increasingly captured by domestic issues. The question becomes can we afford the expanding resources necessary to keep the peace and still answer domestic problems. The final sections of this monograph address the utility of information operations for peace missions. Information operations, the application of the continued advances in information technology, provides a tool to make peace affordable. Information operations allow cost effective solutions.

ACCESSION NUMBER: ADA331354
http://handle.dtic.mil/100.2/ADA331354

Pritulsky, Philip S. ***Strategic Military Communications of the Future: Leveraging Civilian Operations***. Carlisle Barracks, PA: Army War College, March 1998. 53p.

Abstract: The Department of Defense is transiting from a technology driver to a technology rider in strategic communications. Today 95 percent of all military communications travel a portion of their routing via commercial public switched networks. Early in the 21st century, a new generation of commercial

systems will serve as the backbone for all military communications. This extensive leveraging of civilian technology provides tremendous efficiencies for the government. However, with the emergence of the threat of Information Warfare (IW), we must assess the strategic implications of America's reliance on civilian information infrastructures. Does this reliance pose an unacceptable risk to national security. This paper examines the broad implications of military leveraging of strategic communications. It uses the Strategic Principles of War for the 21st Century to assess the impact of this policy on military preparedness.

ACCESSION NUMBER: ADA353653

http://handle.dtic.mil/100.2/ADA353653

Rader, Karl A. ***Blockades and Cyberblocks: In Search of Doctrinal Purity. Will Maritime Interdiction Work in Information Age Warfare?*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1995. 64p.

Abstract: This paper examines the blockade, as both a current concept and a tool suitable to Information Age Warfare. It addresses doctrine's twin demands for precise terminology, to aid shared understanding, and intellectual flexibility, required to win future conflicts. Using joint doctrine, international law, and contemporary practice, the paper examines mixing the military and economic elements of power. Bloodless military coercion, as embodied by maritime interdiction--blockades, embargoes, and quarantines--cannot achieve political ends on its own. It requires the exercise of all elements of national power in order to be effective. The paper applies this finding to information Age warfare, and proposes the doctrinal concept of cyberblock-- the blockade of information transmission media as a Third Wave flexible deterrent option. Like the blockade, the cyberblock cannot necessarily achieve political ends alone. It is a strategic option, utile in the multilateral strategic environment, that relies on all elements of power to coerce international miscreants into compliance with United Nations' behavioral norms. The paper shows that current joint doctrine requires more precise terminology. It further suggests incorporating the term cyberblock as a doctrinal concept that represents an Information Age approach to bloodless military coercion.

ACCESSION NUMBER: ADA301164

http://handle.dtic.mil/100.2/ADA301164

Rattray, Gregory J. ***Strategic Information Warfare: Challenges for the United States***. Wright-Patterson AFB, OH: Air Force Institute of Technology, May 1998. 718p.

Abstract: This work examines the potential for strategic information warfare and the challenges posed for the United States. Strategic information warfare consists of attacks against, and the defense of; information infrastructures for achieving political objectives. My analysis includes consideration of both state and non-state actors. The work focuses on the use of digital means and the cyberspace operating environment for the conduct of such warfare. The first half develops a theoretical basis for addressing strategic information warfare. The work outlines frameworks for the analysis of strategic warfare based on past theories and historical experience. Relying on literature dealing with technology, how it is acquired, assimilated, and diffused, it also creates a framework of factors which facilitate the establishment of organizational technological capability. These frameworks are then applied to the potential offensive and defensive challenges posed by strategic information warfare to identity key areas of concern and uncertainty. The second half undertakes two case studies comparing the development of strategic warfare capabilities. The case studies empirically illustrate the utility of the frameworks across different time periods and types of technologies. The development of air bombardment capabilities by the U.S. and their employment in World War II illustrates the difficulty of creating a new form of strategic warfare. The analysis then details the nascent U.S. effort to develop doctrine, organizations, and technological capability to conduct strategic information warfare in the 1990s, focusing on the defensive aspects of the task. Both case studies rely on primary source material archival materials and accounts of key individuals in the case of strategic bombing; and U.S. military doctrinal publications.

ACCESSION NUMBER: ADA346502

http://handle.dtic.mil/100.2/ADA346502

Rios, Cesar G., Jr. ***Return on Investment Analysis of Information Warfare Systems***. Monterey, CA: Naval Postgraduate School, 2005. 81p.

Abstract: The United States Navy's Cryptologic Carry-On Program Office manages a portfolio of Information Warfare (IW) systems. This research and case study demonstrate how the Knowledge Value Added (KVA) Methodology can be used to formulate a framework for extracting and analyzing performance parameters and measures of effectiveness for each system. KVA measures the effectiveness and efficiency of CCOP systems and the impact they have on the Intelligence Collection Process (ICP) on board U.S. Navy Ships. By analyzing the outputs of the subprocesses involved in the ICP in common units of change, a price per unit of output can be generated to allocate both cost and revenue at the subprocess level. With this level of financial detail, a return on investment (ROI) analysis can be conducted for each process, or asset.

ACCESSION NUMBER: ADA439595

http://handle.dtic.mil/100.2/ADA439595

http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Sep%5FRios.pdf

Scafidi, Anthony L. ***Information Warfare and the Principles of War***. Newport, RI: Naval War College, Joint Military Operations Department, February 1997. 23p.

Abstract: Within all the Services the debate is raging about information dominance, control of 'cyberspace' or the 'Infosphere' and Information Warfare. Some argue that Information Warfare (IW) is just a repackaging of old concepts and current practices, while others contend it is the next Revolution in Military Affairs (RMA). The question that needs to be addressed is; can IW achieve strategic and operational military objectives on its on merit. A way to answer this questions is to analyze IW against our current doctrine. Using the principles of war as a framework, does IW fit (or can it be employed) in the operational environment. Will it be necessary to redefine or update the principles of war to accommodate this changing environment.

ACCESSION NUMBER: ADA325198

http://handle.dtic.mil/100.2/ADA325198

Schechtman, Gregory M. ***Manipulating the OODA Loop: The Overlooked Role of Information Resource Management in Information Warfare***. Wright-Patterson AFB, OH: Air Force Institute of Technology, December 1996. 129p.

Abstract: A ground-swell of interest in information as a weapon of warfare is growing within the U.S. armed services. Military strategists are looking at information as a tool to leverage our forces and make them irresistible in battle. Yet, there is little agreement as to what information warfare (IW) is, let alone how it is best fought. This fundamental disagreement is serving as an impediment to unified actions as the Air Force seeks its role in this arena. In particular, information resource management practitioners are questioning their role in supporting this mission. This thesis discusses limitations of existing information warfare interpretations in light of Col John R. Boyd's decision model, the Observation-Orientation-Decision-Action (OODA) Loop, and offers a synthesized model of information warfare for use in the Air Force. It then offers information resource management (IRM) as a viable decision support mechanism in that interpretation. By analyzing the applicability of information resource management to the Air Force IW mission, this thesis proposes a better way to view information: a tool for winning the information war through making superior decisions more rapidly than our opponents. An understanding of how IRM and IW relate to one another will provide a model for achieving and maintaining dominance of this new realm of warfare.

ACCESSION NUMBER: ADA319636

https://research.maxwell.af.mil/viewabstract.aspx?id=1474

http://handle.dtic.mil/100.2/ADA319636

Schneider, Barry R. and Lawrence E. Grinter. ***Battlefield of the Future: 21st Century Warfare Issues***. Maxwell AFB, AL: Air University, Air War College, September 1998. 277p.

Abstract: This book is about strategy and war fighting in the midst of a revolution in military affairs as the world moves into the twenty-first century. Its 11 essays examine topics such as military operations against a well-armed rogue state or NASTI (NBC-arming sponsor of terrorism and intervention) state; the potential of parallel warfare strategy for different kinds of states; the revolutionary potential of information warfare; the lethal possibilities of biological warfare; and the elements of an ongoing revolution in military affairs (RMA). The book's purpose is to focus attention on the operational problems, enemy strategies, and threats that will confront US national security decision makers in the twenty-first century. The participating authors are either professional military officers or civilian professionals who specialize in national security Issues. Two of the architects of the US air campaign in the 1991 Gulf War have contributed essays that discuss the evolving utility of airpower to achieve decisive results and the lessons that might portend for the future of warfare.

ACCESSION NUMBER: ADA358618

http://handle.dtic.mil/100.2/ADA358618

Schwartzstein, S. J. D. ***Information Revolution and National Security: Dimensions and Directions***. Washington, DC: Center for Strategic and International Studies, c1996. 296p.

Abstract: Information and communications technologies are having a profound impact in a number of ways, domestically and globally, including how national security is maintained and how war is waged. There are also implications for civil liberties and how we, as a society, deal with new kinds of conflict. The issues that are raised are both far-ranging and complex.

See, Judi E. and Gilbert G. Kuperman. ***Information Warfare: Evaluation of Operator Information Processing Models***. Dayton, OH: Logicon Technical Services, Inc., October 1997. 134p.

Abstract: The present document provides a review of 17 models of human information processing. The models were grouped into five classes: Memory and attention, artificial intelligence, visual attention, language comprehension, and situation awareness. The utility of the models was evaluated with respect to their contributions toward understanding the Observe, Orient, Decide, and Act phases of the OODA Loop, the predominant decision making framework for the Third Wave Battlespace, or information warfare. The assessment indicated that current information processing models contribute primarily to the Observe and Orient phases; however, their contributions are disappointingly minor. Further, among the models considered in this review, effective portrayals of the Decide and Act phases were lacking altogether.

REPORT NUMBER: ALCFTR19970166

ACCESSION NUMBER: ADA339749

http://handle.dtic.mil/100.2/ADA339749

Sexton, Joanne. ***Combatant Commander's Organizational View of Information Warfare/Command and Control Warfare***. Newport, RI: Naval War College, June 1995. 33p.

Abstract: Information warfare and Command and Control Warfare (C2W) are widely recognized as describing how the United States will fight its future wars. Of the two, information warfare remains undefined; whereas, C2W is finely detailed and fully defined in joint publications. Despite the inadequate information warfare definition, the combatant commanders have created an Information Warfare/C2W organizational cell built around the five elements of C2W (OP SEC, Deception, PSYOP, EW, and Destruction). From this stepping stone, the combatant commanders will evolve into a more comprehensive strategy to incorporate information warfare. An essential step to this evolution is the need

for the combatant commander to fully understand the ramifications of the following Information Warfare/C2W issues and questions: (1) Why the United States must have a national information policy; (2) What organization should take the lead if the continental United States suffers a devastating, widespread information warfare attack; (3) What is the role of information warfare during peacetime; (4) Who should take the military information warfare lead; (5) Who should have the responsibility to prevent redundant information warfare programs; (6) What should the national security guidance be on black programs; and, (7) How should C2-protect programs be improved. When solved, these seven issues will dictate what future organization and role the military will have in information warfare. The key for the combatant commander is to comprehend these seven issues and seek to shape their solution.

ACCESSION NUMBER: ADA297904

http://handle.dtic.mil/100.2/ADA297904

Smith, Carleton M. ***Logistics Principles in Third Wave Warfare***. Carlisle Barracks, PA: Army War College, April 1999. 47p.

Abstract: In response to a new conceptual world view brought about by the 'Information Age', the Army has committed itself to a course of revolutionary change as it transitions to Army After Next. Already, division redesign initiatives are spreading organizational changes throughout our fighting forces. Transformation of doctrine must proceed apace, challenging whether established principles grounded in past 'Industrial Age' wars can be carried forward through both a revolution in military affairs and an entirely new era of warfare. If logistics truly defines the art of the possible in war, the principles that guide its planning and practice deserve careful scrutiny. This study provides a brief review of current doctrinal logistics principles and explores the ramifications of a trisected world on their status quo. It concludes with a proposal for eight revised logistics principles suitable to Third Wave warfare.

ACCESSION NUMBER: ADA363825

http://handle.dtic.mil/100.2/ADA363825

Smith, Kevin B. ***Crisis and Opportunity of Information War***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1994. 69p.

Abstract: This monograph focuses on the possibility of defeating any and all enemies with an information-intensive force. Clearly, no one currently possesses this capability. However, in the intermediate and long-term, such a force may be within the reach of any post-industrial nation. This monograph explores why this is so, and identifies the major technological 'benchmarks' that must be achieved in order to enable a purely third wave force. Starting with the agrarian notion of the center of gravity, and continuing to the concepts of industrial systems, this monograph will briefly analyze the theories of each of the two preceding 'waves' to determine potential loci of decision. The monograph describes how information systems are starting to form around discrete technological benchmarks that, when eventually integrated, will form a 'knowledge engine' powerful enough to enable commanders to locate and attack the systemic weak point(s) of any enemy. Where possible, case studies will be used to show how this information technology is being used today. Each case study will contain reasonable estimates on where the particular technology involved is trending.

ACCESSION NUMBER: ADA284756

http://handle.dtic.mil/100.2/ADA284756

Staker, R. J. ***Military Information Operations Analysis Using Influence Diagrams and Coloured Petri Nets***. Salisbury, Australia: Electronics Research Laboratory, December 1999. 78p.

Abstract: This report describes how Influence Diagrams, Coloured Petri Net models and related techniques may be used to analyse certain aspects of Military Information Operations. An example is employed to demonstrate these techniques. The example used is a very simplified representation of a Military Command Organisation dealing with a decision problem. The objective of the report is to provide theory, methods and techniques to support the assessment of the effect of Military Information Operations

on such organisations. The simplicity of the example permits the basic concepts to be clearly conveyed. They may readily be extended to the analysis of more complex examples as required. The most fundamental and significant concept developed in this report is that of a common quantitative measure of effectiveness that encompasses all types of Information Operations relevant to Information Warfare. This permits the direct comparison of the effectiveness of alternative Information Operation options with one another and also with conventional operations options. This latter ability is essential if Information Operations are to be employed appropriately as part of a broader range of military options.
REPORT NUMBER: DSTO-TR-0914
ACCESSION NUMBER: ADA373934
http://handle.dtic.mil/100.2/ADA373934

Strategic War ... in Cyberspace. Santa Monica, CA: Rand Corporation, January 1996. 2p.
Abstract: National security is becoming progressively more dependent on and identified with assets related to the 'information revolution.' As part of this revolution, both defense and civilian activities are becoming more heavily dependent on computers and communications, and a variety of key information systems are becoming more densely and extensively interlinked. With the many benefits of the information revolution have also come vulnerabilities. Civilian data encryption and system protection are rudimentary. Talented computer hackers in distant countries may be able to gain access to large portions of the information infrastructure underlying both U.S. economic well-being and defense logistics and communications. Current or potential adversaries may also gain access through foreign suppliers to the software encoded in U.S. transportation and other infrastructure systems. We could thus one day see actions equivalent to strategic attack on targets of national value within the U.S. homeland and on essential national security components and capabilities. In short, there will exist the capability for strategic information warfare.
ACCESSION NUMBER: ADA322533
http://handle.dtic.mil/100.2/ADA322533

Summe, Jack N. ***Information Warfare, Psychological Operations, and a Policy for the Future***. Carlisle Barracks, PA: Army War College, March 1999. 52p.
Abstract: There is a growing interest within DoD concerning the advent of Information Warfare. This interest seems to center around two competing concepts of IW. First is the asymmetrical threat of information-based capabilities used against critical U.S. systems, and second, the burgeoning opportunities that a future Revolution in Military Affairs presents when based on the geometric growth of friendly information-based capabilities. Both analytical tracks seem to indicate that the U.S. must boldly and firmly grasp the potentialities embedded in the growing information age. Yet there are areas within the information environment that have not yet been addressed. Two such areas are a stated National policy for Information Warfare and the future strategic requirements and capabilities for the application of DoD Psychological Operations in support of our new Information Warfare policy. This paper addresses both issues and develops a point of departure for academic dialogue in these two extremely important and sensitive areas.
ACCESSION NUMBER: ADA363817
http://handle.dtic.mil/100.2/ADA363817

Szapranski, Richard. ***Theory of Information Warfare; Preparing for 2020***. Maxwell AFB, AL: Air University, 1995. 12p.
Abstract: THE PROFESSION of arms in a democracy is not exempt from oversight or from consideration of just conduct, even in warfare. Where the will of the people, the moral high ground, and the technological high ground are the same, the profession will remain a useful and lofty one. If, however, the moral high ground is lost, a domino effect occurs: public support is lost, the technological high ground is lost, and the armed forces are lost. It is within this framework that this article postulates a theory of information warfare within the larger context of warfare and proposes ways to wage information warfare at

the strategic and operational levels. The tools to wage information warfare are at hand, and because information weapons are such powerful weapons, both combatants and noncombatants need to be protected against them. The vulnerability to information warfare is universal The decisions to pursue the development of information weapons or to prosecute information warfare are governmental decisions.
ACCESSION NUMBER: ADA328193
http://handle.dtic.mil/100.2/ADA328193

Tait, Steven W. ***The Effects of Budgetary Constraints, Multiple Strategy Selection, and Rationality on Equilibrium Attainment in an Information Warfare Simulation***. Wright-Patterson AFB, OH: Air Force Institute of Technology, 2001. 150p.
Abstract: *Information warfare (IW) has developed into a significant threat to the national security of the United States. Our critical infrastructures are linked together by information systems in a way that is unprecedented in time and is increasingly vulnerable to information attack. However, beneath all the technical means of instigating or defending against such an attack lies the individual decision-maker. This study seeks to understand sum of those factors which affect the ability of an individual to make accurate decisions in an information warfare environment. The study used game theory to analyze the behavior of decision-makers within an IW simulation. The information warfare game model is based on a set of games known as infinitely repeated games of incomplete information. It uses the Bayesian Nashequilibrium concept to determine the strategy which a player should use repeatedly in order to maximize his or her payoff. The results of the experiment show that when a person is faced with increasing numbers of potential strategies, he or she is less likely to make an accurate decision. The results also show that decision-makers that are faced with budgetary constraints and forced to pay for alternative strategies tend to pick those strategies which are most expensive. This is regardless of the actual utility of the strategy as long as it is within the decision-makers' allotted budget. Additionally, the study found that the rationality of the decisions made by an opponent did not significantly affect a player's ability to find the strategy that maximizes his or her own payoff.*
https://research.maxwell.af.mil/viewabstract.aspx?id=3268

Tempestilli, Mark. ***Waging Information Warfare. Making the Connection Between Information and Power in a Transformed World***. Newport, RI: Naval War College, Joint Military Operations Department, May 1995. 47p.
Abstract: This paper discusses the emerging ways, means, and ends of offensive information Warfare (IW). IW is seen as being conducted in a distinctly unique dimension, however, inextricably linked to time, space, and physical force. The context of major geo-social transformation from the proliferation and convergence of powerful information technologies is shown as an underlying theme for change in joint-military operations. The nature of IW is viewed as interwoven in a highly interactive geo-social-technical tapestry- -including various layers of organized conflict (war organisms), represented by an overall system of functional subsystems (physical, mental, spirit). The relationships among physical force, information, and will are deemed essential to leveraging information for appropriate and useful operational effects. The nature of IW and the relationships among the functional subsystems are presented as creating potential for a new level of warfare synergy. Controlling an information continuum of information--knowledge--capability is seen as the key to generating information-based military power. New potential high value target sets are revealed that demand unique understanding and orientation--including a full development of IW beyond the current military interpretation as Command Control Warfare (C2W). A comprehensive view of offensive IW is presented in terms of target development, weaponeering, military options, and organizing for action.
ACCESSION NUMBER: ADA297843
http://handle.dtic.mil/100.2/ADA297843

Thomas, Laurence E., Jr. ***Information Warfare Force XXI Situational Awareness***. Carlisle Barracks, PA: Army War College, March 1998. 44p.

Abstract: The 80's saw the introduction of stovepipe digital architectures in the primary combat arms branches (Aviation, Armor, Artillery, and Infantry) weapon systems. Some of these systems were not interoperable due to their unique software protocols. Aviation and Artillery platforms were interoperable since they utilized the same protocol. In the 90's, General Sullivan expounded on his Force XXI vision to digitally link all the combat arms horizontally and vertically to increase situational awareness. The materiel and combat developments communities produced an internet type system for the combat arms to provide situational awareness. An applique system was installed on some of the platforms so the weapons systems could digitally communicate within the internet. The applique system proposed to solve the stovepipe architectures will not work. Each combat arms system (AH-64D, MlA2 Abrams, M3 Bradley, Paladin/Crusader) has limited space, weight, and power constraints which prevent the integration of the applique system. The Army Acquisition Executive must charter a Project Manager with adequate resources to fully integrate an open architecture system with one operating system tailored into each platform. The Army can not meet the situational awareness objective of Force XXI with another stand alone, federated applique system.

ACCESSION NUMBER: ADA342718

http://handle.dtic.mil/100.2/ADA342718

Thomas, T. R. “InfoWar, InfoTheft, and InfoSec.” Los Alamos National Laboratory, NM: 1993. 3p. IN: ***Workshop on Future Directions in Computer Misuse and Anomaly Detection***. Davis, CA (United States), 31 Mar - 3 Apr 1993.

Abstract: According to its title, the 1993 Davis Computer Security Workshop sponsored by the NSA's Office of INFOSEC (Information Security) and the Air Force's Cryptologic Support Center was suppose to focus on Computer Misuse and Anomaly Detection. No doubt these topics were chosen in response to discussions at the 1992 workshop which clearly identified these areas as critical in the coming year. However, a year in modern computer science is a very, very long time. What was remarkable about this year's meeting was that anomaly detection schemes and misuse models were discussed only to the degree that they were dismissed as irrelevant to the current situation. Rather, the focus this year was on the seriousness and sophistication of the real and potential threats to the integrity of this country's computer-based information systems. This report provides a discussion of information warfare, information theft, and information security.

REPORT NUMBER: LAUR933693, CONF93032361

ACCESSION NUMBER: DE94002700XSP

Thomas, Timothy L. and Cathy Eliot. **Russian and Chinese Information Warfare**: **Theory and Practice**. Fort Leavenworth, KS: Foreign Military Studies Office, 2004. 55p.

Abstract: Russian and China have developed concepts of information operations (IO) and information superiority (IS) that differ from US concepts. Russia divides IO theory into information-technical and information-psychological aspects. According to Rastorguyev, "an information weapon can be any technical, biological, or social means or system that is used for the purposeful production, processing, transmitting, presenting or blocking of data and or processes that work with the data." Effectiveness of disorganizing an enemy's control system determines who will win or lose, even in wars of a limited nature. Chinese General Dai states that "Information operations are a series of operations with an information environment as the basic battlefield condition, with military information and an information system as the direct operational targets, and with electronic warfare and a computer network war as the principal forms; focus is on strength of forces and knowledge." China's focus is on stratagems and control; its IW thinking is evolving away from Western thinking.

ACCESSION NUMBER: ADA467510

http://handle.dtic.mil/100.2/ADA467510

Thompson, Michael J. ***Information Warfare - Who is Responsible? Coordinating the Protection of Our National Information Infrastructure***. Carlisle Barracks, PA: Army War College Strategic Studies Institute, March 1997. 42p.

Abstract: The government of the United States relies on the information Superhighway, officially known as the National Information Infrastructure (NII), to pass critical information. Banking, transportation, communication, medicine, electrical power, and manufacturing are also dependent upon the NII to pass the information required for them to operate. The U.S. Military depends on the NII for the movement of personnel and equipment, voice and data communications and research and development. The nation's power is provided through the national power grid which is connected to the NII. The NII is vulnerable to intrusion, disruption and exploitation by hackers, hostile entities, or anyone with a modest amount of automation equipment. Leadership at the national level is required to coordinate government and private sector actions to ensure the security and reliability of the NII.

ACCESSION NUMBER: ADA326536

http://handle.dtic.mil/100.2/ADA326536

Thrasher, Roger D. ***Information Warfare: Implications for Forging the Tools***. Monterey, CA: Naval Postgraduate School, June 1996. 160p.

Abstract: One part of the modern Revolution in Military Affairs (RMA) is the possibility of a new form of warfare-often called information warfare. Development of information warfare depends on technological advances, systems development and adaptation of operational approaches and organizational structures. This thesis assesses the implications of information warfare for the technology and systems development areas, with the underlying motivation of ensuring the military is postured to win the information warfare RMA through effective research, development and acquisition. This assessment takes place primarily through a 'Delphi' process designed to generate discussion between selected information warfare experts about the impacts of information warfare. This thesis concludes that information warfare is largely dependent on commercial information technology. This dependence means the military should rely on the commercial sector for most technological advances and products-with government research funds focused on military-unique research areas. Use of commercial items, coupled with DoD standard architectures, may enable a decentralization of information warfare acquisition to the user level. Finally, this dependence means the acquisition system should focus on architecture development, technology insertion, systems integration and on managing functions and services of systems-primarily through development of operational software to run on mostly commercial hardware.

ACCESSION NUMBER: ADA311887

http://handle.dtic.mil/100.2/ADA311887

Treadwell, Mark B. ***When Does an Act of Information Warfare Become an Act of War: Ambiguity in Perception***. Carlisle Barracks, PA: Army War College, May 1998. 47p.

Abstract: There is no clear-cut point where information operations can cross over to become the decisive point leading to the start of armed conflict. The use of information operations by nations and individuals could have a significant impact on the public opinion, and, by extension, on the leaders of a nation. Traditional acts of war have been directed towards events that influence a nation's access to, use of, or benefit from land. How these concepts may be extended to information, either historical (archived or stored) or real-time (systems in use), is problematic at best. This paper addresses how information warfare may be interpreted by nations and private citizens in this context.

ACCESSION NUMBER: ADA345572

http://handle.dtic.mil/100.2/ADA345572

Uchida, Ted T. ***Building a Basis for Information Warfare Rules of Engagement***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, December 1997. 67p.

Abstract: The U.S. armed forces face a global information threat which could launch an attack without warning. This surprise attack could damage the U.S. armed forces ability to mobilize, deploy and control forces worldwide. The attack will use the global information infrastructure to target the information based processes the U.S. armed forces utilize to dominate the entire spectrum of conflict. To protect information based processes, U.S. armed forces joint operational planners are building plans to defeat and possibly attack information based threats. This monograph discusses how the U.S. armed forces should regulate the defensive and offensive responses to information attack with Rules of Engagement. After defining several terms, this monograph illustrates the gravity of the threat the U.S. armed forces face in the information spectrum. The proliferation of computers and networking is creating a huge underclass of IW warriors bent on destroying, manipulating, and stealing information. While past IW threats were curious 'hackers,' the modem IW environment is encompassed by over 18 countries currently pursing active IW attack and defense programs. Dealing with a threat requires operational planners recognize that information is rapidly becoming the center of gravity for military operations. This monograph proposes IW planners build IW ROE that extends maximum protection to information by protecting key information systems and infrastructure. Additionally, IW ROE should also allow the U.S. armed forces to autonomously implement retaliatory or pre-emptive self defensive actions to counter any information based threat.

ACCESSION NUMBER: ADA340230
http://handle.dtic.mil/100.2/ADA340230

_____. ***Domestic Information Warfare: The Department of Defense's Role in the Civil Defense of the National Information Infrastructure***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies. May 1998. 82p.

Abstract: Now more than ever every facet of society relies on the NII to facilitate critical information related activities. Entities around the world have not ignored this transformation and seek to steal, disrupt, and interdict the U.S.'s key information processes. It is this reliance on the NII and the security threats it faces that force policy makers to answer the question who should protect the NII. Seemingly, the DoD is well positioned to take the lead role in protecting the NII. However, authorizing DoD control over NII protection ignores many issues. Analyzing vulnerabilities to the DII illustrates the gravity of the problem the entire NII faces. The NII faces an increasing threat from hackers, and rogue agents bent on damaging the DoD's information based processes. Countering these threats requires developing a comprehensive NII protection strategy. Correspondingly, developing a strategy for protecting the NII requires defining several strategic concepts of Centers of Gravity, objective, end state, and key tasks. Along with strategic concepts, several critical environmental paradigms such as changing mediums of warfare and the source of future power also effect decisions of who should protect the NII. In light of environmental paradigms and strategic concepts, the issue of whether the DoD can serve as lead agent in NII protection begins to take shape. While arguments such as experience in matters related national security appear to point toward the DoD playing the central role in NII protection, the underlying rationale is limiting and shortsighted. The NII's distributed nature, constitutionally mandated rights, and the needs of a pluralistic society, all argue against the DoD playing a lead role in protecting the NII. While the DoD should not play the lead role, it does have the capacity to take leadership in several key sub-task areas. First, the DoD should be the l.

ACCESSION NUMBER: ADA357866
http://handle.dtic.mil/100.2/ADA357866

Vadnais, Daniel M. ***Law of Armed Conflict and Information Warfare--How Does the Rule Regarding Reprisals Apply to an Information Warfare Attack?*** Maxwell AFB, AL: Air Command and Staff College, 1997 34p.

Abstract: The question of how to characterize an information warfare attack, particularly what is known as a "hacker attack,: has not been fully developed. It must be, though, in order to understand how a nation can respond to it. This paper explores applicable tenets of international law. It identifies various methods of engaging in the spectrum of activities known as information warfare, and then discusses the one that has been underexplored in the context of a military response. Finally, it addresses the applicability of the law of armed conflict to a "hacker attack." Given that during wartime, almost any means of imposing one belligerent's will on another is legitimate, subject to the various tenets international law, the question that needs to be addressed is what range of activities is permissible during times other than war, when parties are not engaged in traditionally understood applications of armed force." The current body of international law seems to mitigate against including hacking" in the definition of armed force," the standard necessary for unilateral military armed reprisal actions. In that case, unless the initial attack rises to the level that would permit some action by the "victim" in self-defense, that nation is relegated to seeking action from the United Nations Security Council.

ACCESSION NUMBER: ADA392890
http://handle.dtic.mil/100.2/ADA392890

Vandewart, Ruthe L. and Richard L. Craft. “Analytic Tools for Information Warfare.” p. 58-68, IN: ***Proceedings of the 1996 Command and Control Research and Technology Symposium.*** Monterey, CA: Naval Postgraduate School, 25-28 June 1996. Washington, DC: National Defense University, 1996. 876p.

Abstract: Information warfare and system surety (tradeoffs between system functionality, security, safety, reliability, cost, usability) have many mechanisms in common. Sandia's experience has shown that an information system must be assessed from a (ital system) perspective in order to adequately identify and mitigate the risks present in the system. While some tools are available to help in this work, the process is largely manual. An integrated, extensible set of assessment tools would help the surety analyst. This paper describes one approach to surety assessment used at Sandia, identifies the difficulties in this process, and proposes a set of features desirable in an automated environment to support this process.

REPORT NUMBER: CONF-96-061702; SAND-96-0484C
ACCESSION NUMBER: DE96010856

Walter, Kevin R. ***Strategic Leadership's Role in Information Warfare***. Carlisle Barracks, PA: Army War College, May 1998. 50p.

Abstract: This study examines the appropriate role of strategic leadership in the development of a National Information Strategy and supporting policies. It examines current policy and evaluates its reliance on information technology as a means to implement the policy. It offers a history of the Internet, a look at its accelerated growth, and its relevance to national interest. It concludes by arguing for a coherent, effective National Information Strategy and supporting policies to carry the country into a new millennium.

ACCESSION NUMBER: ADA348139
http://handle.dtic.mil/100.2/ADA348139

Wang, Ken. ***Information Warfare Targeting: People and Processes***. Monterey, CA: Naval Postgraduate School, 2003. 67p.

Abstract: Information Warfare targeting has long been a crucial, but unrecognized, part of military operations. From Sun Tzu's targeting of the enemy's will to fight, to today's information-centric warfare, it is those who have understood the techniques and applications of Information Warfare targeting who have most often prevailed. As critical as it is to our success, it is a topic that is controversial, often

misunderstood, and subject to various interpretations. This thesis examines the IW targeting process, consisting of people, information, systems, and the interaction between the function of targeting and IW. In the Information Age, IW has been recognized as viable warfare area. However, IW targeting cannot be treated as traditional targeting utilized by other warfare areas. This thesis is intended to serve as a guide for the study of this topic and provides an instructional program designed to satisfy the requirement for a coherent instructional program on IW Targeting. IW targeting affects every facet of warfare and in turn is affected by these facets. In preparing for a future that calls for maximizing the effects while minimizing the effort, it is critical that we understand the process in order to remain effective.

ACCESSION NUMBER: ADA420637

http://handle.dtic.mil/100.2/ADA420637

http://bosun.nps.edu/uhtbin/hyperion-image.exe/03Dec%5FWang.pdf

Ward, Thomas E., III. ***Information Warfare: Is It Feasible? Desirable?*** Carlisle Barracks, PA: Army War College, March 1996. 38p.

Abstract: *Information Warfare is a hot topic throughout the Department of Defense today, and a debate rages about what it really is, who the warfighters are, and what its impact will be on warfare in the future. This study defines key concepts of information warfare, examines its offensive and defensive components, and compares information warfare to a previous technological revolution, air warfare. The paper draws on a broad spectrum of resources from military, philosophy, business, and computer-oriented perspectives. It examines opportunities and potential pitfalls in the conduct of offensive and defensive information warfare, the desirability and feasibility of using information warfare weapons and techniques, and concludes with precautionary caveats about vulnerabilities, expectations, and applicability.*

ACCESSION NUMBER: ADA309292

http://handle.dtic.mil/100.2/ADA309292

Weidner, James H. ***People Side of Information Warfare***. Newport, RI: Naval War College, June 1996. 32p.

Abstract: *Whether at the strategic, operational or tactical level of war, success has become directly related to getting the right information to the right person at the right time. Information-based technologies have permitted orders-of-magnitude increases in the speed at which information can be transmitted, processed, and accessed. Always a concern when dealing with such potentially large quantities of real-time information is the problem of information overload of the users. That will be the impact of this information flow on the individuals at the human-machine interface. Recently, a few notable authors have expressed reservations about the promises of information warfare. Interestingly, those reservations center on issues related to getting enough talented people to serve as information warriors. This paper examines some of the issues related to the people side of information warfare. Arguably, the real center of gravity is not information but rather the information warriors themselves. The challenge will be, as it has always been, to ensure that we have enough talented individuals to get the job done.*

ACCESSION NUMBER: ADA312077

http://handle.dtic.mil/100.2/ADA312077

Wells, David, et al. ***Survivability in Object Service Architectures (OSA*)**. Baltimore, MD: Object Services and Consulting Inc., October 1999. 167p.

Abstract: *The military of the future will increasingly rely upon information superiority to dominate the battlespace. The size and complexity of the software systems necessary to achieve this goal makes them highly vulnerable to the loss or degradation of hosts, networks, or processed due to physical and information warfare attacks, hardware and infrastructure failures, and software errors. This report summaries the goals and results of a project that developed an architecture and software mechanisms to make military and commercial software applications based on the popular Object Services Architecture (e.g., OMG's CORBA) model far more survivable than is currently possible, while at the same time maintaining the flexibility and ease of construction that characterizes OSA based applications.*

ACCESSION NUMBER: ADA372229
http://handle.dtic.mil/100.2/ADA372229

Whisenhunt, Robert H. ***Information Warfare and the Lack of a U.S. National Policy***. Carlisle Barracks, PA: Army War College, April 1996. 30p.
Abstract: The information technology explosion is having a profound impact on the Information Infrastructure of the United States. This has led to growing national security problems for government agencies as well as private industry. The problems are not totally new, but the speed at which technology allows information processes to take place has raised their relative importance in the conduct of daily commerce. The greatest return on investment appears to be in the area of improved defensive capabilities of our networks. Many agencies and departments (government and private industry) are working on the problem independently. Cooperation and coordination are either unlikely or will take far too long. The best approach is a policy statement from the Executive Branch that places the responsibility on a single agency or committee to integrate these fragmented efforts into a coherent program for national security.
ACCESSION NUMBER: ADA309392
http://handle.dtic.mil/100.2/ADA309392

White, Kenneth C. ***Cyber-Terrorism: Modem Mayhem***. Carlisle Barracks, PA: Army War College, April 1998. 40p.
Abstract: America can no longer rely on broad oceans and a strong military to protect its homefront. The arrival of the information age has created a new menace cyber terrorism. This threat recognizes no boundaries, requires minimal resources to mount an attack, and leaves no human footprint at ground zero. This study addresses technology, identification procedures, and legal ambiguity as major issues, for countering cyber terrorism as an emerging challenge to U.S. national security. As America's reliance on computer technology increases, so does its vulnerability to cyber attacks.
ACCESSION NUMBER: ADA345705
http://handle.dtic.mil/100.2/ADA345705

Whitehead, YuLin G. ***Information as a Weapon. Reality Versus Promises***. Maxwell AFB, AL: Air University, School of Advanced Airpower Studies. January 1999. 46p.
Abstract: The concept of information warfare (IW) continues to gain visibility within political and military arenas in the United States. Active discourse by individuals in the government and private circles regarding what constitutes the proper emphasis on and employment of IW indicates the subject is still shrouded in controversy. In the simplest terms, literature on the role of information war exists in two categories: as information in warfare and as information warfare. The former discusses information in the more traditional notion of a support for decision making and combat operations. The latter, however, uses information as a weapon in and of itself in warfare. This thesis addresses the second theme and questions whether information is a weapon. The author employs the theories and principles of Carl von Clausewitz as a theoretical underpinning for critical analysis. The study investigates whether information as a weapon can achieve the purposes of war. Specifically, can the use of the 'information weapon' diminish an adversary's will and capacity to fight. The results indicate that while information may be considered a weapon, it is one that must be used with caution. The more enthusiastic proponents of the information weapon tend to overestimate it's ability to diminish enemy will and capacity to fight. In fact, three characteristics of IW, as envisioned by its proponents, are particularly unconvincing. They describe the information weapon as a low-cost weapon with a high payoff, a method to eliminate the fog and friction of war for friendly forces yet enshroud the enemy in the same, and as a tool to attain quick and bloodless victories. Several implications and cautions result from this study's analysis regarding the use of the information weapon. Information is not a technological 'silver bullet,' able to subdue the enemy without battle.
ACCESSION NUMBER: ADA360997

http://www.au.af.mil/au/database/research/ay1997/saas/whitehead_yg.htm
http://www.au.af.mil/au/database/projects/ay1997/saas/whitehead_yg.pdf

Wood, Robert J. ***Information Engineering the Foundation of Information Warfare***. Maxwell AFB, AL: Air University, Air War College, April 1995. 79p.

Abstract: If information is governed by physical laws, information engineering may be possible. If information engineering is possible, it forms the basis for developing information weapons. Thus information engineering is the foundation of information warfare. This paper establishes the theoretical linkage between the potentially new discipline of information engineering and the activities that could encompass information warfare. The focus of this paper is on applying the lessons from other engineering disciplines and the body of physics and physical knowledge to the field of information warfare. The study of information engineering begins by modeling the ways in which individuals process information. Once the information engineer understands the model for individual information processing, the engineer can use the model to illuminate some of the vulnerable aspects of group and mass processing of information. Knowing the physics of information enables the information engineer to better understand and apply appropriate tools in twenty-first century information warfare.

ACCESSION NUMBER: ADA329024

Ihttp://www.au.af.mil/au/database/research/ay1995/awc/woodrj.htm
http://www.au.af.mil/au/database/projects/ay1995/awc/woodrj.pdf

Wright, Beverly C. ***Information Warfare: Measures of Effectiveness***. Newport, RI: Naval War College, May 1999. 23p.

Abstract: Information warfare (IW) has become central to the way nations fight wars and technological advances on the horizon will only increase the importance of IW to the operational commander. The growing significance of IW requires the development of measures for determining its effectiveness. This paper specifically explores measures of effectiveness for C2-attack. Measuring the effectiveness of C2-attack actions is critical to the operational commander because effective C2-attack allows a commander to gain the initiative, thereby establishing and maintaining a primary advantage over an adversary. Since it is important to align measures of effectiveness with mission objectives or goals, possible measures of effectiveness are developed for each of the four goals of C2-attack. Developing meaningful measures of effectiveness for C2-attack is quite a challenge due to its significant subjective content. The dilemma is how to combine objective and subjective measures so the commander has a complete picture. In many respects, objective measures can be rolled up into an overall subjective measure. Some measures, however, just don't quantify well. As a commander plans a specific action and then implements that action, it is imperative he be able to measure the effectiveness of that action, analyze the results of that measurement, and then finally use the results of that analysis to plan the next action. Mastering this process may very well be one of the greatest challenges of command.

ACCESSION NUMBER: ADA370688
http://handle.dtic.mil/100.2/ADA370688

Wright, Larry. ***Information Warfare and Cyber Defense.*** McLean, VA: Booz-Allen and Hamilton, Inc., 2002. 46p.

Abstract: These viewgraphs discuss information warfare and cyber defense. Massive networking has made the U.S. the world's most vulnerable target for information attack. Public and private infrastructure have become virtually indistinguishable and largely global.

ACCESSION NUMBER: ADA406363
http://handle.dtic.mil/100.2/ADA406363

Ye, Nong. ***The Monitoring, Detection, Isolation and Assessment of Information Warfare Attacks Through Multi-Level, Multi-Scale System Modeling and Model Based Technology.*** Tempe, AZ: Arizona State University, 2004. 150p.

Abstract: With the goal of protecting computer and networked systems from various attacks, the following intrusion detection techniques were developed and tested using the 1998 and 2000 MIT Lincoln Lab Evaluation Data: Exponentially Weighted Moving Average techniques for autocorrelated and uncorrelated data to detect anomalous changes in the audit event intensity; a learning and inference algorithm based on a first-order Markov chain model of a normal profile for anomaly detection; two multivariate statistical process control techniques based on chi-square and Canberra distance metrics for anomaly intrusion detection; the technique of probabilistic networks with undirected links to represent the symmetric relations of audit event types during normal activities, build a long-term profile of normal activities, and then perform anomaly detection; and Decision tree techniques to automatically learn intrusion signatures, and to classify information system activities into normal or intrusive for producing useful intrusion warning information. Finally, this report presents a research prototype of an Intrusion Detection System (IDS) integrating the intrusion detection techniques and a process model of a computer and network system.

ACCESSION NUMBER: ADA421322

http://handle.dtic.mil/100.2/ADA421322

Yoshihara, Toshi. ***Chinese Information Warfare: A Phantom Menace or Emerging Threat.*** Carlisle Barracks, PA: Army War College, 2001. 51p.

Abstract: The author explores what he perceives to be China s pursuit of information warfare (IW) as a method of fighting asymmetric warfare against the United States. He believes the Chinese are seeking ways to adapt IW to their own style of warfare. Paradoxically, he observes that the Chinese have not gleaned their intelligence through espionage, but through careful scrutiny of U.S. IW in practice. The author examines those aspects of IW--PSYOPS, Denial, and Deception--that China believes provides the greatest prospects for victory in a conflict. Not surprisingly, Sun Tzu is interwoven into this emerging theory. Targeting the enemy's nervous system at all levels, that is, his ability to gather and assess information and then transmit orders, provides significant advantages in the prosecution of a campaign. He concludes that the extent of Chinese advances or intent regarding IW is difficult to ascertain given its closed society. Chinese IW may still be nascent, but the menacing intent is there and only vigilance will protect the United States.

ACCESSION NUMBER: ADA397266

http://handle.dtic.mil/100.2/ADA397266

http://www.carlisle.army.mil/ssi/pubs/display.cfm/hurl/PubID=62

DKL U163 .Y68 2001 GENERAL

Information Operations

Books

Allard, Ken. “Information Operations in Bosnia.” p. 599, IN: **Proceedings of the Third International Symposium on Command and Control Research and Technology.** National Defense University, Washington, DC, 17-20 June 1997. Washington, DC: National Defense University, 1997. 893p.
DKL UB212 .I573 1997 GENERAL

Allen, Patrick D. **Information Operations Planning.** Norwood, MA: Artech House, c2007. 323p.
DKL U163 .A44 2007 GENERAL

Armistead, Leigh (ed.). **Information Operations: Warfare and the Hard Reality of Soft Power.** Dulles, VA: Brassey's, 2004. 277p.
Original available at *http://www.iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf*
DKL U163 .I52 2004 GENERAL

Bailey, Timothy J., Robert A. Claflin and Roland R. Groover. “Information Operations in Force-on-Force Simulations.” p. 744-770, IN: **Proceedings of the 1996 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 25-28 June 1996. Washington, DC: National Defense University, 1996. 876p.
DKL UB212 .C68 1996 GENERAL

Bansemer, John D. **Meeting the Joint Vision 2020 Challenge: Organizing for Information Operations.** Maxwell AFB, AL: Air University, Air Command and Staff College, 2001. 46p.
https://research.maxwell.af.mil/viewabstract.aspx?id=3599

Bartley, Richard and Kurt A. Richardson. “Analysis Framework for Information Operations.” p. 918-921, IN: **Proceedings of the 1998 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 29 June - 1 July 1998. Washington, DC: National Defense University, 1998. 943p.
DKL UB212 .C68 1998 GENERAL

Bass, Carla D. **Building Castles on Sand? Ignoring the Riptide of Information Operations**. (Maxwell paper, no. 15) Maxwell AFB, AL: Air University, Air War College, 1998. 46p. *http://www.au.af.mil/au/awc/awcgate/maxwell/mp15.pdf*

Blackington, Robert E. **Air Force Information Operations (IO) Doctrine: Consistent With Joint IO Doctrine?** Maxwell AFB, AL: Air University, Air Command and Staff College, 2001. 53p.
https://research.maxwell.af.mil/viewabstract.aspx?id=3558

Bunker, Robert J. **Information Operations and the Conduct of Land Warfare**. Land Warfare Paper no. 31. Arlington, VA: Institute of Land Warfare, Association of the United States Army, 1998. 21p.

Campen, Alan D. **Cyberwar 3.0: Human Factors in Information Operations and Future Conflict.** Fairfax, VA: AFCEA International Press, 2000. 309p.
DKL UA23 .C93 2000 GENERAL

Gaines, Robert J. **Future Information Operations (IO) in the Military: Is It Time for an "IO CINC?"** Maxwell, AFB, AL: Air University, Air Command and Staff College, 2000. 23p.
https://research.maxwell.af.mil/viewabstract.aspx?id=2081

Glock, John R. **Operationalizing Information Operations.** Maxwell, AFB, AL: Air University, Air Command and Staff College, 2000. 38p.
https://research.maxwell.af.mil/viewabstract.aspx?id=2083

Issler, Gordon D. **Space War Meets Info War: The Integration of Space and Information Operations.** Maxwell, AFB, AL: Air University, Air Command and Staff College, 2000. 12p.
https://research.maxwell.af.mil/viewabstract.aspx?id=3312

Larsen, Wayne A. **Serbia Information Operations During Operation Allied Force.** Maxwell, AFB, AL: Air University, Air Command and Staff College, 2000. 37p.
https://research.maxwell.af.mil/viewabstract.aspx?id=2090

Lindner, Blake F. **Information Operations: America's Plan for Strategic Failure**. Maxwell AFB, AL: Air University, Air War College, 1998. 41p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1812

Munipalli, Seshagiri. **Information Operations: Moving from Doctrine to Execution**. Maxwell AFB, AL: Air University, Air Command and Staff College, 1999. 45p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1984

Osborne, William B., et al. **Information Operations: A New War-Fighting Capability**. Maxwell AFB, AL: Air University, Air Command and Staff College, 1996. 65p.
http://csat.au.af.mil/2025/volume3/vol3ch02.pdf

Proceedings of the 8th International Command and Control Research and Technology Symposium. "Track 7 Information Superiority/Information Operations." National Defense University, Washington, DC, 17-19 September 2003. Washington, DC: National Defense University, 2003.
http://www.dodccrp.org/events/8th_ICCRTS/Tracks/track_7.htm

Proceedings of the 9th International Command and Control Research and Technology Symposium. "Track 8.1 Information Superiority/Information Operations." Copenhagen, Denmark, 14-16 September 2004. Washington, DC: National Defense University, 2004.
http://www.dodccrp.org/events/9th_ICCRTS/CD/foreword.htm

Proceedings of the 10th International Command and Control Research and Technology Symposium. "Track 7 Information Operations/Assurance." Vienna, VA, 13-16 June 2005. Washington, DC: National Defense University, 2005.
http://www.dodccrp.org/events/10th_ICCRTS/CD/foreword.htm

Proceedings of the 2000 Command and Control Research and Technology Symposium. "Track 6 Information Operations." Naval Postgraduate School, Monterey, CA, 26 June – 28 June 2000. Washington, DC: National Defense University, 2000.
http://www.dodccrp.org/events/2000_CCRTS/index.htm

Proceedings of the 2001 Command and Control Research and Technology Symposium. "Track 7 Information Superiority/Information Operations." US Naval Academy, Annapolis, MD, 19 June – 21 June 2001. Washington, DC: National Defense University, 2001.
http://www.dodccrp.org/events/6th_ICCRTS/index.htm

Proceedings of the 2002 Command and Control Research and Technology Symposium. "Track 7 IS/IO." Naval Postgraduate School, Monterey, CA, 11-13 June 2002. Washington, DC: National Defense University, 2002.
http://www.dodccrp.org/events/2002_CCRTS/fore.htm

Proceedings of the 2004 Command and Control Research and Technology Symposium. "Track 3 Information Superiority/Information Operations", San Diego, CA, 15-17 June 2004. Washington, DC: National Defense University, 2004.
http://www.dodccrp.org/events/2004_CCRTS/CD/foreword.htm

Seinwill, Jeffrey D. **Organizing Joint Forces for Information Operations: The Viability of a Joint Force Information Operations Component Commander**. Maxwell AFB, AL: Air University, Air Command and Staff College, 1999. 44p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1959

Swentkofske, Virginia G. **Planning and Conducting Offensive Counterinformation Operations**. Maxwell AFG, AL: Air University, Air War College, 2002. 46p.
https://research.maxwell.af.mil/viewabstract.aspx?id=4722

Taylor, Donald P. and Wayne Lacey. **Task Force Eagle Information Operations: Tactics, Techniques, and Procedures.** Newsletter (Center for Army Lessons Learned (U.S.) ; no. 03-18. Fort Leavenworth, KS: Center for Army Lessons Learned (CALL), U.S. Army Training and Doctrine Command (TRADOC), 2003.

Contents: 1. Information operations (IO) -- 2. IO in Bosnia and Herzegovina -- 3. IO mission essential task list (METL) -- 4. IO team -- 5. Synchronization matrix development -- 7. IO operational rhythm, overview -- 8. Talking points -- 9. IO analysis; tactics, techniques and procedures and lessons learned.
DKL D 101. 22/25:03-18 FEDDOCS

Thomas, Timothy L. **Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations**. Conflict Studies Research Centre, Royal Military Academy, Sandhurst Foreign Military Studies Office, 1997. 19p. *http://www.iwar.org.uk/iwar/resources/call/98-21toc.htm*

Tulak, Arthur N. **Task Force Eagle Information Operations: "IO in a Peace Enforcement Environment."** [Newsletter (Center for Army Lessons Learned); No. 99-2.] Fort Leavenworth, KS: Center for Army Lessons Learned, 1999. 86p.

_____. **Task Force Eagle Tactics, Techniques, and Procedures (TTPs) for Information Operations: Lessons Learned and Unit-Level TTPs** . [Newsletter (Center for Army Lessons Learned); No. 99-15.] Fort Leavenworth, KS: Center for Army Lessons Learned, 1999. 76p.

United States. Army War College. **Information Operations Primer.** Carlisle Barracks, PA: Army War College, 2006. 158p.
http://www.carlisle.army.mil/usawc/dmspo/Publications/Information%20Operations%20Primer%20AY07%20(30%20Nov%2006).pdf
OR http://www.iwar.org.uk/iwar/resources/primer/info-ops-primer.pdf

United States. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. **Information Operations**. [Washington, DC]: Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Dept. of Defense, [199?]

United States. Defense Science Board. **Protecting the Homeland Defense Information Operations.** Washington, DC: Defense Science Board, 2001 [various parts]
Vol. 1 – http://www.acq.osd.mil/dsb/reports/protecting.pdf
Vol. 2 – http://www.acq.osd.mil/dsb/reports/dio.pdf
Vol. 2, pt. 2 -- http://www.acq.osd.mil/dsb/reports/2001-06-DIO_Vol_II_Part_2.pdf

United States. Department of the Army. Headquarters, Training and Doctrine Command. **Concept for Information Operations**. TRADOC Pamphlet 525-69, Fort Monroe, VA: TRADOC, 1 August 1995.
http://www.tradoc.army.mil/tpubs/pams/p525-69.htm

United States. Department of the Army. Office of the Deputy Chief of Staff for Operations and Plans Information Operations Division. **Information Operations**. Washington, DC: U.S. Dept. of the Army, Office of the Deputy Chief of Staff for Operations and Plans, [1996?] 17p.

United States. Department of Defense, **Information Operations.** Department of Defense Directive 3600.1. Washington, DC: Department of Defense, 9 December 1996.

United States. Department of Defense. **Information Operations Roadmap**. Washington, DC: Department of Defense, 2003. 74p.
http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf

United States. Joint Chiefs of Staff. **Joint Doctrine for Information Operations**. Joint pub ; 3-13 [Washington, D.C.]: Joint Chiefs of Staff, 1998.
http://www.iwar.org.uk/iwar/resources/us/jp3_13.pdf

United States. Joint Chiefs of Staff. **Joint Doctrine for Information Operations**. Joint pub ; 3-13 [Washington, D.C.]: Joint Chiefs of Staff, 2006.
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

United States. Joint Forces Staff College. **Joint Information Operations Handbook**. Norfolk, VA: Joint Forces Staff College, 2002.
http://www.iwar.org.uk/iwar/resources/jiopc/io-handbook.pdf

United States. Joint Forces Staff College. **Joint Information Operations Handbook**. Norfolk, VA: Joint Forces Staff College, 2003.
http://www.iwar.org.uk/iwar/resources/jiopc/io-handbook-2003.pdf

Westwood, C. J. **Military Information Operations in a Conventional Warfare Environment**. Air Power Studies Centre Paper No. 47. Canberra, Australia: Royal Australian Air Force. Air Power Studies Centre, August 1996. 35p.

White, Randall L. **Command & Control Structures for Space and Information Operations in a Joint Command**. Maxwell AFB, AL: Air University, Air Command and Staff College, 2002. 37p.
https://research.maxwell.af.mil/viewabstract.aspx?id=4724

Periodicals

Ackerman, Robert K. “Information Operations Absorb Traditional Service Activities.” **Signal**, March 2000, v. 54, no. 7, p. 23-26.

_____. “Infowarriors Ensure Local Citzenry Gets the Message.” **Signal**, March 2002, v. 56, no. 7, p. 20-21.

_____. “Technology Empowers Information Operations in Afghanistan.” **Signal**, March 2002, v. 56, no. 7, p. 17-20.

Algermissen, Robert M, et al. "Task Force Eagle Information Operations Planning." **News From the Front!**, March/April 1999.

Allan, Charles T. “Electronic Warfare: Foundation of Information Operations.” **Journal of Electronic Defense**, October 1998, v. 21, no. 10, p. 59-64+

Allard, Kenneth. "Information Operations in Bosnia: A Preliminary Assessment." **Strategic Forum**, November 1996, no. 91.
http://www.ndu.edu/inss/strforum/SF_91/forum91.html

Anderson, Matt, Joel Hamby and Frank O’Donnell. “Battalion/Task Force Targeting and the Military Decision-Making Process (MDMP) in the Information Operations (IO) Environment.” **Combat Training Center (CTC) Quarterly Bulletin**, 1st Quarter FY 2000, no. 00-4.

Baker, Ralph O. “The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations.” **Military Review**, May/June 2006, v. 86, no. 3, p. 13-32.
http://usacac.army.mil/CAC/milreview/English/MayJun06/webpdf/Baker.pdf

Barnett, Roger W. "Information Operations, Deterrence, and the Use of Force." **Naval War College Review**, Spring 1998, v. 51, no. 2, p. 7-19.

Bass, Carla. “Building Castles on Sand: Understanding the Tide of Information Operations.” **Airpower Journal**, Summer 1999, v. 13, no. 2, p. 27-45.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/sum99/bass.html OR
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/sum99/bass.pdf

Batschelet, Allen W. “Information Operations for the Joint Warfighter.” **Field Artillery**, July-August 2004, p. 8-10.
http://sill-www.army.mil/FAMAG/2004/JUL_AUG_2004/Pages8-10.pdf

Beavers, Garry J. “Defining the Information Campaign. **Military Review**, November/December 2005, v. 85, no. 6, p. 80-82.
http://usacac.army.mil/CAC/milreview/download/English/NovDec05/keeton.pdf

Billigmeier, Scott and Ed Glabus. “Future War: 'Information Operations Corps' Comes of Age.” **Army**, December 1997, v. 47, no. 12, p. 45-50.

Bloom, Bradley. “Information Operations in Support of Special Operations.” **Military Review**, January-February 2004, v. 84, no. 1, p. 45-49.
http://usacac.army.mil/CAC/milreview/English/JanFeb04/JanFeb04/bloom.pdf

Bosch, J.M.J. “Information Operations--Challenge or Frustration?” **Military Technology**, May 2000, v. 24, no. 5, p. 86-89.

Boyd, Curtis D. “Army IO is PSYOP: Influencing More with Less.” **Military Review**, May/June 2007, v. 87, no. 3, p. 67-75.
http://usacac.army.mil/CAC/milreview/English/MayJun07/Boyd.pdf

Boyd, Morris J. and Michael Woodgerd. “Information Operations: Force XXI Operations.” **Military Review**, November 1994, v. 74,no. 11, p. 17-28.

Brown, Robin. “Information Operations, Public Diplomacy & Spin: The United States & the Politics of Perception Management.” **Journal of Information Warfare**, 2002, v. 1, no. 3, p. 40-50.
http://ics.leeds.ac.uk/papers/pmt/exhibits/32/JIW1_32.pdf

Bunker, Robert J. “The Future of War.” **Military Review**, November/December 1999, v. 79, no 6, p. 76-77.

_____. “Information Operations and the Conduct of Land Warfare.” **Military Review**, September-November 1998, v. 78, no. 5, p. 4-17.

Campen, Alan D. “Information Operations May Find Definition and Validation in Iraq.” **Signal**, June 2003, v. 57, no. 10, p. 43-45.

_____. “Information Operations Seeks Blend of Missives and Missiles.” **Signal**, June 2002, v. 56, no. 10, p. 33-35.

_____. “Intelligence Is the Long Pole in The Information Operations Tent.” **Signal**, March 2000, v. 54, no. 7, p. 35-36.

Colestock, Trent R. “Company FSO's IO Experience in OIF II.” **Field Artillery**, September- October, 2005, v. 5, no. 5, p.38-39.
http://sill-www.army.mil/FAMAG/2005/SEP_OCT_2005/SEP_OCT_05_Page_38_39.pdf

Cormier, Ken. “DSB Task Force Evaluates Information Operations in Bosnia.” **Journal of Electronic Defense**, May 1997, v. 20, no. 5, p. 54+.

Cosumano, Joseph M., Jr. “Space, Missile Defense and Information Operations Support the Transforming Army.” **Army**, 2002-03 Green Book, October 2002, v. 52, no. 10, p. 187-194.

Curtis, Steven, Robert, et al. “Integrating Targeting and Information Operations in Bosnia.” **Field Artillery**, July-August 1998, p. 31-36.
http://sill-www.army.mil/FAMAG/1998/JUL_AUG_1998/JUL_AUG_1998_FULL_EDITION.pdf

Darley, William M. “Clausewitz's Theory of War and Information Operations.” **Joint Force Quarterly: JFQ**. First Quarter 2006, no. 40, p. 73-79.
http://www.dtic.mil/doctrine/jel/jfq_pubs/4015.pdf

_____. “Strategic Imperative: The Necessity for Values Operations as Opposed to Information Operations in Iraq and Afghanistan.” **Air & Space Power Journal**, Spring 2007, v. 21, no. 1, p. 33-41.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/spr07/darleyspr07.html

_____. “Why Public Affairs Is Not Information Operations.” **Army**, January 2005, v. 55, no. 1, p. 9-10.

Davis, Norman C. "Information Operations and the Marine Corps Planning Process." **Marine Corps Gazette**, August 1998, v. 82, no. 8, p. 56-63.

_____. "The Marine Corps and Information Operations." **Marine Corps Gazette**, April 1997, v. 81, no. 4, p. 16-22.

Dearth, Douglas H. “Critical Infrastructures and the Human Target in Information Operations.” **Journal of Information Warfare**, December 2001, v. 1, no. 2, p. 62-67.

_____. “Implications and Challenges of Applied Information Operations.” **Journal of Information Warfare**, 2001, v. 1, no. 1, p. 7-15.

_____. “Shaping the Information Space.” **Journal of Information Warfare**, 2002, v. 1, no. 3, p. 1-15.
http://ics.leeds.ac.uk/papers/pmt/exhibits/32/JIW1_32.pdf

Delaney, Kevin M., et al. “Health Information Operations: Improving What the AMEDD Communicates.” **Journal of the U.S. Army Medical Department**, January-March 2004, v. 1, no. 1, p. 6-9.

Denying the Enemy: A Concept for Information Operations.” **Surface Warfare**, July-August, 1998, v. 23, no. 4, p. 22-27.

Dhillon, Joginder S. and Robert I. Smith. “Defensive Information Operations and Domestic Law: Limitations on Government.” **Air Force Law Review**, 2001, v. 50, p. 135-174.

DiCenso, David J. “Information Operations: An Act of War?” **Law Technology**, 2nd Quarter 2000, v. 33, no. 2, p. 26-44.

“Doctrinal Information Operations Issues.” **Military Intelligence Professional Bulletin**, July-September 1999, v.25, no. 3, p. 53-55.

Donskov, Yu Ye and O. G. Nikitin. “Special Information Operations in Armed Conflicts.” **Military Thought**, 2005, v. 14, no. 3, p. 33-38.

Dowell, Cody D., Marc J. Romanych and Jerry M. Carter. “Joint Task Force Information Operations.” **Cyber Sword**, Fall 1999, v. 3, no. 1, p. 6-9.

Driscoll, Susan C. “Who’s in Control?: Contemporary Audience –Media Relations and Their Implications for Perception Management.” **Journal of Information Warfare**, 2002, v. 1, no. 3, p. 65-71.
http://ics.leeds.ac.uk/papers/pmt/exhibits/32/JIW1_32.pdf

Duczynski, Guy. “Getting to Purposeful Information Operations: The Application of Effects-Based Approaches.” **Journal of Information Warfare**, 2006, v. 4, no. 3.

Dunne, Jonathan P. "Tactical Information Operations.” **Marine Corps Gazette**, September 2006, v. 90, no. 9, p. 78,80

Emery, Norman. “Fighting Terrorism and Insurgency: Shaping the Information Environment.” **Military Review**, January-February 2005, v. 85, no. 1, p. 32-38.

_____. “Information Operations in Iraq.” **Military Review**, May-June 2004, v. 84, no. 3, p. 11-14.
http://usacac.army.mil/cac/milreview/download/English/MayJun04/emery.pdf

_____. Intelligence Support to Information Operations: Staff Chaplains.” **Military Intelligence Professional Bulletin**, July-September 2003, v. 29, no. 3, p. 19-21.
http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=269&issueID=19

Emery, Norman E., Rob S. Earl, & Raymond Buettner. “Terrorist Use of Information Operations.” **Journal of Information Warfare**, June 2004, v. 3, no. 2, p. 34-45.

Ferris, John. “A New American Way of War? C4ISR, Intelligence and Information Operations in Operation 'Iraqi Freedom': A Provisional Assessment.” **Intelligence & National Security**, Winter 2003, v. 18, no. 4, p. 155-174.

_____. “Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?” **Intelligence and National Security**, Summer 2004, v. 19, no. 2, p. 199-225.

Flynn, Michael T. “Understanding Our Future Battlespace: Why We Need to Integrate IO Into the IPB Process.” **Military Intelligence Professional Bulletin**, October-December 2001, v. 27, no. 4, p. 25-29.
http://www.universityofmilitaryintelligence.us/mipb/archives/v27n4.pdf

Fogleman, Ronald R. "Information Operations: The Fifth Dimension of Warfare." **Defense Issues**, 1995, v. 10, no. 47, p. 1-3.
http://www.defenselink.mil/speeches/speech.aspx?speechid=936

"Force XXI Information Operations." **Military Review**, May-June 1995, v. 75, no. 3, p. 38.

Franz, Timothy P., et al. “Defining Information Operations Forces: What Do We Need?” **Air & Space Power Journal**, Summer 2007, v. 21, no. 2, p. 53-63+
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/sum07/franz.html

Fulghum, David A. “Cyberwar Plans Trigger Intelligence Controversy.” **Aviation Week & Space Technology**, January 19, 1998, v. 148, no. 3, p. 52-54.

Garfield, Andrew. “The Offence of Strategic Influence: Making the Case for Perception Management.” **Journal of Information Warfare**, 2002, v. 1, no. 3, p. 30-39.
http://ics.leeds.ac.uk/papers/pmt/exhibits/32/JIW1_32.pdf

Geraci, Richard V. and W. David Reese. “Army Transformation War Game: Space, Missile Defense and Information Operations. “ **Army**, February 2003. v. 53, no. 2, p. 35-38.

Glenister, Cynthia A. “Information Operations in the IBCT (Interim Brigade Combat Team). “ **Military Review**, May-June 2002, v. 82, no. 3, p. 59-62.
http://usacac.army.mil/CAC/milreview/English/MayJun02/MayJun02/glen.pdf

Gourley, Scott R. “Information Operations and FM 100-6 and FM 3-14: Guides to the Information Age.” **Army**, April 2001, v. 51, no. 4, p. 21-23.

Grange, David L. and James A. Kelley. "Information Operations for the Ground Commander." **Military Review**, March/April 1997, v. 77, no. 2, p. 5-12.

Grazzini, Christopher P. “Information Operations by the British in the War of 1812 During the Maryland Campaign.” **Defense Intelligence Journal**, 2003, v. 12, no. 2, p. 29-41.

Grohoski, David C., Steven M. Seybert and Marc J. Romanych. “Measures of Effectiveness in the Information Environment.” **Military Intelligence Professional Bulletin**, July-September 2003, v. 29, no. 3, p. 12-16. *http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=267&issueID=19*

Guenther, Eric and Gary Schreckengost. “Converting the IO Concept into Reality.” **Armor**, July-August 2003, v. 112, no. 4, p. 18-20+

Guevin, Paul R. “Information Operations.” **Air & Space Power Journal**, Summer 2004, v. 18, no. 2, p. 122. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj04/sum04/guevin1.html*

Hall, Wayne M. “Information Operations (IO): Military Competition.” **Cyber Sword**, Spring 2000, v. 4, no. 1, p. 6-10.

Hanson, Lynn. “Organization of the Information Operations Cell for a Joint Task Force.” **Cyber Sword**, Spring 2000, v. 4, no. 1, p. 29-31.

Hasenauer, Heike. “Understanding Information Operations.” **Soldiers**, October 2006, v. 61, no. 10, p. 20-23. *http://www.army.mil/publications/soldiersmagazine/pdfs/oct06all.pdf*

Hellwig, Frederick C. and Boyd R. Plessl. “Defending Information Operations at the Joint Task Force**.” INSCOM Journal for the Military Intelligence Professional**, Spring 2001, v. 24, no. 2, p. 22-23.

Hellwig, Frederick C. and Thaddeus A. Dmuchowskli “Army Develops Innovative Solution for Information Operations Training.” **Defense Intelligence Journal**, 2003, v. 12, no, 1, p. 87-95.

Hill, Greg W. and Rob Meyer. “Role of Religion in Information Operations.” **Army Chaplaincy**, Summer-Fall 2002, v. 2, no. 2, p. 54-57.

Hill, Joel H. “Transforming Intelligence Education to Support Information Operations.” **Defense Intelligence Journal**, 2003, v. 12, no, 1, p. 97-100.

Hobson, Sharon. "Canada's Information Ops in Defensive Role: The Canadian Forces are Reshaping their Information Operations Capabilities." **Jane’s Defence Weekly**, October 15, 1997, v. 28, no. 15, p. 29-30.

Howle, Timothy E. “Information Operations: The Role of Civil-Military Operations and Civil Affairs.” **Special Warfare**, Spring 1997, v, 10, no. 2, p. 16-17.

Hubbard, Zachary P. “Information Operations and Information Warfare in Kosovo: A Report Card We Didn’t Want to Bring Home.” **Cyber Sword**, Spring 2000, v. 4, no. 1, p. 27-29.

_____. “IO (Information Operations) in the Information Age.” Part 1: The Genesis and Evolution of Joint IO and Part 2. IO in the U.S. Air Force. **Journal of Electronic Defense**, Part 1, April 2004, v. 27, no. 4, p. 51-57; Part 2, May 2004, v. 27, no. 5, p. 49-52.

“Information Operations.” **Marine Corps Gazette**, August 1998, v. 82, no. 8, p. A1-A10.

“Information Operations.” **Military Review**, November 1994, v. 74, no. 11, p. 16.

“Information Operations.” **Military Review**, September/November 1998, v. 78, no. 5, p. 18.

"Information Operations." **Military Review**, November/December 1995, v. 75, no. 6, p. 2.
"Information Operations." **Military Review**, November/December 1996, v. 76, no. 6, p. 2.

“Information Operations Absorb Traditional Service Activities.” **Signal**, March 2000, v. 54, no. 7, p. 23-26.

“Information Operations Center Provides Attack-Thwarting Tools.” **Signal**, July 1998, v. 52, no. 11, p. 26+

Jajko, Walter. “A Critical Commentary on the Department of Defense Authorities for Information Operations.” **Comparative Strategy**, April-June 2002, v. 21, no. 2, p. 107-114.

Johnson, Karlton, D. “Rethinking Joint Information Operations.” **Signal**, October 2002, v. 57, no. 2, p. 57-59.

Jones, Craig S. "The Information Operations Process." **News From the Front!**, March/April 1998.

_____. “The Perception Management Process.” **Military Review**, December 1998 – February 1999, v. 78, no. 6, p. 38-43.

Jones, Kristyn E. “Counter-Intelligence/Human Intelligence Support to Information Operations.” **INSCOM Journal for the Military Intelligence Professional**, April-June 1998, v. 21, no. 2, p. 10-13.

Jones, Synthia S., Bernard Flowers and Karlton D. Johnson. “Unity of Effort in Joint Information Operations.” **Joint Force Quarterly**, Winter 2002-03, no. 33, p. 78-83. *http://www.dtic.mil/doctrine/jel/jfq_pubs/1433.pdf*

Josten, Richard J. “IO Support to the CINC.” **Cyber Sword**, Fall 1999, v. 3, no. 1, p. 10-13.

Kagan, Frederick W. “Star Wars in Real Life: Political Limitations of Space Warfare.” **Parameters**, Autumn 1998, v. 28, no. 3, p. 112-120.
http://carlisle-www.army.mil/usawc/Parameters/98autumn/kagan.htm

Kasales, Michael C. “The Reconnaissance Squadron and ISR Operations.” **Military Review**, May/June 2002, v. 82, no. 3, p. 52-58.
http://usacac.army.mil/CAC/milreview/English/MayJun02/MayJun02/kasales.pdf

Keeton, Pamela and Mark McCann. “Information Operations, STRATCOM, and Public Affairs.” **Military Review**, November/December 2005, v. 85, no. 6, p. 83-86.
http://usacac.army.mil/CAC/milreview/download/English/NovDec05/keeton.pdf

Knowles, John. "A Wider View and a Bigger Bite: EW (Electronic Warfare) in Information Operations." **Journal of Electronic Defense**, October 1997. v. 20, no. 10, p 51-57.

Kuehl, Dan. “Defining Information Power.” **Strategic Forum**, June 1997, no. 115, p. 1-5.
http://www.ndu.edu/inss/strforum/SF115/forum115.html

LaBahn, Timothy D. “Information Operations in Bosnia.” **Field Artillery**, November-December 2001, p. 28-33.
http://sill-www.army.mil/FAMAG/2001/NOV_DEC_2001/NOV_DEC_2001_PAGES_28_33.pdf

Lamb, Christopher J. “Information Operations as a Core Competency.” **Joint Force Quarterly**, 2004, no. 36, p. 88-96.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1536.pdf

Laughridge, Gene. “Recent and Not-So-Recent Thinking on Information Operations and the Knowledge of War.” **Army Communicator**, Spring/Summer 1995, v. 20, no. 2, p. 32-38.

Lawlor, Maryann. “Information Operations Specialists Move to Mission Planners' Table.” **Signal**, December 2005, v. 60, no. 4, p. 47-50.

Levesque, Laura A. “Intelligence Support to Information Operations: Open Source Intelligence Operations at the Division Level.” **Military Intelligence Professional Bulletin**, October-December 2005, v. 31, no. 4, p. 55-57.
http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=142&issueID=6

Lev, Lzhar. “ Information Operations and Counterterrorism.” **Jane’s Intelligence Review**, September 2002, v. 14, no. 9, p. 50-53.

Macklin, James. “Information Operations and the Law: A Practical Guide for Signal Planners and Operators.” **Army Communicator**, Fall 1999, v. 24, no. 3, p. 12-16.

Madigan, James C. and George E. Dodge. “Battle Command: A Force XXI Imperative.” **Military Review**, November 1994, v. 74, no. 11, p. 29-39.

Magnan, Stephen W. “Safeguarding Information Operations [Are We Our Own Worst Enemy?].” **Studies in Intelligence**, Summer 2000, v. 46, no. 9, p. 97-104.
https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v44i3a08p.htm
OR
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art08.html

Maiers, Mark W. and Timothy L. Rahn. “Information Operations and Millennium Challenge.” **Joint Force Quarterly**, 2004, no. 35, p. 83-87.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1635.pdf

McConville, James E. “U.S. Army Information Operations: Concepts and Execution.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 17-22.

McCrohan, Kevin F. “Competitive Intelligence: Preparing for the Information War.” **Long Range Planning**, August 1998, v. 31, no. 4, p. 586-593.

McFate, Montgomery. “Manipulating the Architecture of Cultural Control: A Conceptual Model for Strategic Influence Operations in North Korea.” **Journal of Information Warfare,** March 2005, v. 4, no. 1, p. 21-40.

McGinley, James E. “Information Operations Planning: A Model for the Marine Air-Ground Task Force.” **Marine Corps Gazette**, September 2001, v. 85, no. 9, p. 48+

McNeive, James F. “Information Operations at the Tactical Level.” **Marine Corps Gazette**, June 2003, v. 87, no. 6, p. 52-53.

“Megabytes Join Muddy Boots in U.S. Army Force Operations.” **Signal**, March 2000, v. 54, no. 7, p. 31-33.

Metz, Thomas F. “Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations.” **Military Review**, May/June 2006, v. 86, no. 3, p. 2-12.
http://usacac.army.mil/CAC/milreview/English/MayJun06/webpdf/Metz.pdf

“Military Leaders Formulate Virtual Organization Plan.” **Signal**, March 2000, v. 54, no. 7, p. 27-29.

Miller, Michael G. “Information Operations Planning for 2000 and Beyond: The Joint IO Planning Process and IO Navigator.” **Cyber Sword**, Spring 2000, v. 4, no. 1, p. 10-13.

Mize, Randy. “Revised Air Force Doctrine Document 2-5, Information Operations.” **Air & Space Power Journal**, Summer 2005, v. 19, no. 2, p. 36.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/sum05/notam1.html

Morton, Jason L. “CI (Counterintelligence) in Information Operations: Enabling Operators and Defining Emerging Roles for CI in Army IO (Information Operations). **Military Intelligence Professional Bulletin**, July-September 2003, v. 29, no. 3, p. 36-37+
http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=273&issueID=19

Murphy, Dennis M. “Information Operations on the Nontraditional Battlefield.“ **Military Review,** November-December 1996, v. 76, no. 6, p. 16-18.

Nelson, Bradford K. “Applying the Principles of War in Information Operations.” **Military Review**, September-November 1998, v. 78, no. 5, p. 31-35.

Nelson, Scott. “The Algerian Six: Lessons-Learned From Information Operations.” **Defense Intelligence Journal**, 2003, v. 12, no, 1, p. 67-77.

Newell, Mark R. “Tactical-Level Public Affairs and Information Operations.” **Military Review**, December-February 1998-1999, v. 78, no. 6, p. 21-28.

Nicander, Lars. “Information Operations – A Swedish View.” **Journal of Information Warfare**, 2001, v. 1, no. 1, p. 16-24.

Notar, Charles E. “Information Operations (IO) and Its Implications on the Five Functions of the Military Police.” **Military Police**, Winter 1999, v. 99, no. 1, p. 16-22.

Nowak, Leonard G. “Information Operations and the IBCT [Interim Brigade Combat Team].” **Military Review**, September-October 2000, v. 80, no. 5, p. 35-38.

Nunn, Matthew J. ASAS (All-Source Analysis System) Master Analysts’ Support to Information Operations.” **Military Intelligence Professional Bulletin**,
Pt. 1 – Information Engineering – July-September 2003, v. 29, no, 3, p. 64.
http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=285&issueID=19
Pt. 2 -- Communications – October-December 2003, v. 29, no. 4, p. 71
http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=238&issueID=17
Pt. 3 – Analysis – January-March 2004, v. 30, no. 1, p. 78.
http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=216&issueID=16

O’Brien, Kevin and Izhar Lev.” Information Operations and Counterterrorism.” **Jane’s Intelligence Review**, September 2002, v. 14, no. 9, p. 50-53.

Paschall, Joseph F. “IO for JOE: Applying Strategic IO at the Tactical Level.” **Field Artillery**, July-August 2005, v. 5, no. 4, p. 25-29. *http://sill-www.army.mil/FAMAG/2005/JUL_AUG_2005/PAGES25_29.pdf*

_____. “Tactical Information Operations in Operation Iraqi Freedom.” **Marine Corps Gazette**, March 2004, v. 88, no. 3, p. 56-59.

Peasley, Mark D. “Force XXI: USAIC&FH Support to Information Operations.” **Military Intelligence Professional Bulletin**, October-December 1996, v. 22, no. 4, p. 51.

Pounder, Gary. “Opportunity Lost: Public Affairs, Information Operations, and the Air War in Serbia.” **Air & Space Power Journal**, Summer 2000, v. 19, no. 2, p. 56-78. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/sum00/pounder.pdf* OR *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/sum00/pounder.htm*

Pullen, Randy. “Army Reserve Taking Initiative to Battle Computer Hacking.” **Army Reserve Magazine**, Fall 1998, v. 44, no. 2, p. 23.

Raduege, Harry, Jr. “Defensive Information Operations: A J-6 Perspective.” **Army Communicator**, Fall 1998, v. 23, no. 4, p. 55-57.

Raschall, Joseph F. “Tactical Information Operations in Operation IRAQI FREEDOM.” **Marine Corps Gazette**, March 2004, v. 88, no. 3, p. 56-59.

Rhodes, J.E. “A Concept for Information Operations.” **Marine Corps Gazette**, August 1998, v. 82, no. 8, p. A1-A10 [Insert].

Robins, Bill. "Implications of Information Age Operations." **RUSI Journal**, October 1997, v. 142, no. 5, p. 32-39.

Robins, W. J. P. "Information Age Operations." **RUSI Journal,** June 1997, v. 142, no. 3, p. 37-41.

Robinson, Clarence A., Jr. "Army Information Operations Protect Command and Control." **Signal**, July 1996, v. 50, no. 11, p. 47-50.

_____. "Deft Federal Burglar Alarms Receive Funding Jump-Start." **Signal**, March 2000, v. 54, no. 7, p. 17-21.

_____. “Information Operations Center Provides Attack-Thwarting Tools.” **Signal**, July 1998, v. 52, no. 11, p. 26.

_____. “Information Operations Sweep Across Milieu of Peace and War.” **Signal**, September 1999, v. 54, no. 1, p. 47-50.

Romanych, Marc J. and Kenneth Krumm. “Tactical Information Operations in Kosovo.” **Military Review**, September/October 2004, v. 84, no. 5, p. 56-61. *http://usacac.army.mil/cac/milreview/download/English/SepOct04/roman.pdf*

Schellhammer, Mike. “Information Operations: Part of Full-Spectrum Battlefield.” **INSCOM Journal for the Military Intelligence Professional**, Winter, 2001, v. 24, no. 1, p.21-22.

Schreckengost, Gary J. and Gary A. Smith. “IO in SOSO at the Tactical Level: Converting Brigade IO Objectives into Battalion IO Tasks**.” Field Artillery**, July-August 2004, v. 4, no. 3, p. 11-15. *http://sill-www.army.mil/FAMAG/2004/JUL_AUG_2004/Pages11-15.pdf*

Schulte, Gregory L. “Deterring Attack: The Role of Information Operations.” **Joint Force Quarterly**, Winter 2002-03, no. 33, p. 84-89. *http://www.dtic.mil/doctrine/jel/jfq_pubs/1533.pdf*

Scott, William B. “International Space Assets, ‘Information Ops' Seen as Key Elements in Conducting Future Combat Operations.” **Aviation Week & Space Technology**, December 8, 1997, v. 147, no. 23, p 26.

Seffers, George I. “Information Operations go on the Offensive.” **Air Force Times**, November 23, 1998, v. 59, no. 16, p. 30.

_____. “Services to Link Efforts to Track Hackers.” **Army Times**, April 27, 1998, v. 58, no. 39, p. 28.

_____. “Task Force Will Combat Hackers.” **Air Force Times**, April 27, 1998, v. 58, no. 38, p. 28.

Sessions, William S. "The FBI's Strategic Information Operations Center." **The Police Chief**, December 1989, v. 56, no. 12, p. 10+

Shanahan, Stephen W. and Garry J. Beavers. "Information Operations in Bosnia." **Military Review**, November-December 1997, v. 77, no. 6, p. 53-62.

Shaw, John. “Does the JFC Need a JIOTF? Strengthening IO Doctrine.” **Cyber Sword**, Fall 1999, v. 3, no. 1, p. 4-6.

Sholtis, Tadd. “Public Affairs and Information Operations: A Strategy for Success.” **Air & Space Power Journal**, Fall 2005, v. 19, no. 3, p. 97-106. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/fal05/sholtis.html*

Sieting, Lori, A. “Doctrine Corner: Intelligence Support to Information Operations: Today and in the Objective Force.” **Military Intelligence Professional Bulletin**, July-September 2003, v. 29, no. 3, p. 56-60. *http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=283&issueID=19*

Sizer, Richard A. “Land Information Warfare Activity: IO and IW Support to Army XXI.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 23-24.

Skopowski, Paul. “Information Operations and the Marine Corps.” **Marine Corps Gazette**, February 2002, v. 86, no. 2, p. 39-42.

Souder, Jeff. “Army Pictorial Service’s Films as Information-Operations Tool in World War II.” **Army Communicator**, Fall 2001, v. 26, no. 3, p. 47-53.

Starry, Michael D. and Charles W. Arneson, Jr. “FM (Field Manual) 100-6: Information Operations.” **Military Review**, November-December 1996, v. 76, no. 6, p. 3-15.

Stern, Matthew A. and Steven M. Seyber. "'This is What I'm Thinking About....' A (Theoretical) Tactical Commander Gives His IO Guidance." **News From the Front!** July/August 1999.

Stahl, Pamela M. and Toby Harryman. “Center for Law and Military Operations (CLAMO) Report.” **The Army Lawyer**, March 2004, p. 30-38.

Swart, William R. “Modeling & Simulation Essential Ingredient for Successful Information Operations.” **Cyber Sword**, Fall 1997, v. 1, no. 2, p. 10-12.

Szeredy, J "Spyke." “Influence Operations: Integrated PSYOP Planning.” **Air & Space Power Journal**, Spring 2005, v. 19, no. 1, p. 38-44. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/spr05/szeredy.html*

Taylor, Phillip M. “Perception Management and the ‘War’ Against Terrorism.” **Journal of Information Warfare**, 2002, v. 1, no. 3, p. 16-29. *http://ics.leeds.ac.uk/papers/pmt/exhibits/32/JIW1_32.pdf*

Terry, James P. “Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What at the Targeting Constraints?” **Military Law Review**, September 2001, v. 169, no. 1, p. 70-91.

Thomas, Timothy L. "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations." **Journal of Slavic Military Studies**, March 1998, v. 11, no. 1, p. 40-62. Also published as CALL Publication #98-21.

_____. “Russian Information Operations Bibliography.” **Low Intensity Conflict & Law Enforcement**, Summer 1997, v. 6, no. 1, p. 205-215.

Tolle, Glenn A. “Shaping the Information Environment.” **Military Review**, May-June 2002, v. 82, no. 3, p. 47-49. [IO]
http://usacac.army.mil/CAC/milreview/English/MayJun02/MayJun02/tolle.pdf

Tomlin, Greg. “More than a Campaign of Platitudes: Effective Information Operations for the Battalion/Task Force and Company/Team.” **Armor**, May/June 2006, v. 115, no. 3, p. 20-25+

Trent, Stoney and James L. Doty, III. “Marketing: An Overlooked Aspect of Information Operations.” **Military Review**, July-August 2005, v. 85, no. 4, p. 70-74.
http://usacac.army.mil/CAC/milreview/download/English/JulAug05/trent.pdf

Tulak, Arthur N. “Information Operations in Support of Demonstrations and Shows of Force.” **Call Training Techniques**, FY99, 2nd Quarter and **News From the Front!** November/December 1989 and **Military Intelligence Professional Bulletin**, July-September 2003, v. 29, no. 3, p. 9-11.
http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=267&issueID=19

_____. "Physical Destruction Component of Information Operations in Peace Enforcement. " **News From the Front!**, September/October 1998.

_____. "PSYOP C2W Information Operations in Bosnia." **News From the Front!**, November/December 1998.

Tulak, Arthur N., Kelly R. Broome and Donnie S. Bennett “The Evolution of Information Operations at Brigade and Below.” **Military Review**, March-April 2005, v. 85, no. 2, p. 18-23.

Tulak, Arthur N. and James E. Hutton. “Information System Components of Information Operations.” **Military Review**, September-November 1998, v. 78, no. 5, p. 19-25.
http://usacac.army.mil/CAC/milreview/download/English/MarApr05/tulak.pdf

Tyndall, William and Tim Mishkofski. “Information Operations Training Focuses on Agility.” **Signal**, June 2005, v. 59, no. 10, p. 65-67.

Walker, Regina. “Overview of Information Operations Condition (INFOCON).” **Cyber Sword**, Spring 2000, v. 4, no. 1, p. 17-20.

Wells, C. J. “Information Superiority & Support: Misplaced & Misunderstood.” **Journal of Information Warfare**, March 2005, v. 4, no. 1, p. 49-60.

Wilde, Andy. “Update: Information Operations.” **A Common Perspective**, October 1998, v. 6, no. 2, p. 7-10.
http://www.dtic.mil/doctrine/jel/comm_per/acp6_2.pdf

Williams, Greg. “Information Operations in the Army Reserve: USAR Needs Soldiers With High-Tech Skills to Fill Units and Positions Nationwide.” **Army Communicator**, Winter 2000, v. 25, no. 4, p. 14-15.

Wood, C. Norman. “Information Operations Change the Map of Conflict.” **Signal**, March 2000, v. 54, n. 7, p. 14.

Wright, Richard H. “Information Operations: Doctrine, Tactics, Techniques and Procedures.” **Military Review**, March-April 2001, v. 81, no. 2, p. 30-32. *http://usacac.army.mil/CAC/milreview/English/MarApr01/MarApr01/wright.pdf*

Documents, Theses & Technical Reports

Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography.

Aiken, Scott D. ***Marine Air-Ground Task Force Offensive Information Operations, Supporting Operational Maneuver from the Sea.*** Fort Leavenworth, KS: Army Command and Staff College, 2000. 147p.

Abstract: The Marine Air-Ground Task Force (MAGTF) is the organizational structure that the Marine Corps will continue to use to task organize forces. The Marine Corps must prepare doctrine to meet the challenges and opportunities that Information Operations (IO) offers. The challenges and opportunities of IO are only now beginning to be defined by the Marine Corps. Currently, there is no Marine Corps doctrine to assist MAGTF personnel in the conduct of offensive IO. This thesis proposes thirteen doctrinal principles for the employment of the elements of offensive IO for a forward deployed MAGTF operating in a littoral, unformed or developing operational environment. These proposed doctrinal principles support Operational Maneuver From the Sea and provide a link between the 1998 Marine Corps Concept Paper A Concept for Information Operations and actual operating procedures. These proposed doctrinal principles are more specific than current Joint doctrine. This thesis also proposes several recommendations for the implementation of these principles into procedure. The documentary (historical) method and the case studies, based on successful historical examples of operations in the littorals from World War II to the present, are used.

ACCESSION NUMBER: ADA383920

http://handle.dtic.mil/100.2/ADA383920

Ball, Charles R. ***Decision Aids and Wargaming for Information Operations***. Carlisle Barracks, PA: Army War College, April 1999. 47p.

Abstract: Information operations are an essential component of our current and future warfighting strategy as outlined in the latest National Military Strategy and Joint Vision 2010. Simulations such as WARSIM 200 are an important enabler that will permit us to train for and execute this strategy. However, information operations are not included in any current simulation nor are they addressed in any automated decision aids supporting these simulations. The Defense Advanced Research Projects Agency developed a constraint based decision aid to support Course of Action Analysis (COAA) for simulation support at the School of Advanced Military Studies. This decision aid can be extended to represent information operations courses of action. This SRP recommends changes to the decision aid to support the Electronic Warfare (EW) component of Information Operations. It also describes example constraints that can be used to represent the EW component of a division attack scenario. Finally, it recommends a strategy for adding information operations components to joint and army warfighting simulations and for extending the COAA program to address campaign level planning.

ACCESSION NUMBER: ADA363158

http://handle.dtic.mil/100.2/ADA363158

Bansemer, John D. ***Meeting the Joint Vision 2020 Challenge: Organizing for Information Operations.*** Maxwell AFB, AL: Air University, Air Command and Staff College, 2001. 54p.

Abstract: Joint Vision 2020 recognizes the increasing importance of operations within the information domain as well as the need to have appropriately designed organizations prepared to support and conduct operations within the information domain This paper provides an initial framework to assess organizational structures for IO using the evolution of British and American airpower organizations during the interwar years This analysis will show how, over time, the debate over organizing air forces became centered on a core set of criteria, Applying these criteria to IO will provide a preliminary determination of the degree of organizational autonomy warranted for IO, In a similar manner, the organizational decisions made during the interwar years had direct implications on both airpower and service organizations These implications will be assessed against three organizational constructs: an independent IO service, semi-autonomous service organizations, and a joint unified command This analysis will illustrate that an independent service is not warranted at this time; however, it does point to a requirement to grant greater autonomy to IO organizations within the services to help foster operational and doctrinal innovation, Finally, a pre-existing joint unified command should assume control of all IO capabilities to ensure the proper integration of the many disparate capabilities grouped under the IO rubric.

ACCESSION NUMBER: ADA406958

http://handle.dtic.mil/100.2/ADA406958

Bass, Carla D. ***Building Castles on Sand? Ignoring the Riptide of Information Operations***. Maxwell AFB, AL: Air University, Air War College, September 1998. 53p.

Abstract: This paper postulates that the information operations (IO) mission should be centralized at the unified command level, specifically Atlantic Command (ACOM), to capture the plethora of uncoordinated, IO related activities ongoing throughout DOD. Using Special Operations Command (SOCOM) as a model, ACOM would assign teams to combatant commands to help plan and execute information operations missions. ACOM should be allocated a program element (PE) for information operations, paralleling SOCOM's major force program IO. This would alleviate a major criticism identified in several national level studies regarding insufficient, sporadic, and uncoordinated IO expenditures. Establishing an information operations PE would also minimize the conflict with conventionally minded elements of DOD that resist realigning kinetic resources to fund IO initiatives, another problem identified at the national level. Designated as commander in chief for information.

ACCESSION NUMBER: ADA356005

http://handle.dtic.mil/100.2/ADA356005

_____. ***Global Engagement: Building Castles On Sand?*** Maxwell AFB, AL: Air University, Air War College, April 1998. 59p.

Abstract: From the earliest ages, technological innovations shaped strategies and tactics, often resulting in new eras in military operations. Proliferation of technology, exemplified by computers and sensors, challenges civilian and military decision makers and military leaders to understand radical changes associated with the information age, and capabilities and vulnerabilities associated therewith. Information Operations (IO) challenges traditional, conceptual, and operational approaches to borders, boundaries, and sovereignty. Title 10 and Goldwater-Nichols currently define military organizations, structure, functions, and influence organizational evolution. In this context, how should the US organize for IO? Is a new or non-traditional organizational structure needed to address IO? How might relationships within the Intelligence Community and with the DoD be affected? Identify, define, evaluate the range of potential policy constraints (e.g., tradition, doctrine, regulation, public law) on IO that civilian and military decision makers confront in planning and implementing IO campaigns? Examine ongoing research detailing US Information Infrastructure...what are the most pressing "Achilles' Heels?" How can US leverage technologies, organizations, concept of operations, and strategies to fend off threats to our infrastructure?

https://research.maxwell.af.mil/viewabstract.aspx?id=1791

Beckno, Brian T. ***Preparing the American Soldier in a Brigade Combat Team to Conduct Information Operations in the Contemporary Operational Environment.*** Fort Leavenworth, KS: Army Command and Staff College, 2006. 103p.

Abstract: This thesis examines whether the Army is adequately preparing its tactical leaders and soldiers in Brigade Combat Teams (BCT) to conduct Information Operations (IO) in the Contemporary Operational Environment (COE). First, an explanation of IO and its Army applicability is presented using current examples from military operations in Operation Iraqi Freedom (OIF). While conducting counterinsurgency (COIN) operations in Iraq, IO has become a critical combat enabler because of its nonlethal ability to influence adversarial, foreign friendly, and neutral audiences. Second, the author identifies select IO skills and IO applications in which American soldiers in a BCT should be trained to effectively conduct IO within a BCT. The skills are intercultural communication, language, negotiation, and media awareness. The applications are laws of war, rules of engagement, ethics and morality, and commander's intent. Third, the thesis examines the Army's institutional education and operational training of IO at the BCT level and below. Using institutional course management plans from select officer and noncommissioned officer schools and current operational training directives for deploying units to Iraq, an analysis of IO education and training was conducted. The thesis concludes with recommendations to the institutional and operational Army for improving IO education and training for American soldiers serving in a BCT.

ACCESSION NUMBER: ADA451276

http://handle.dtic.mil/100.2/ADA451276

Bishop, Roy V. ***Information Operations: A Layman's Perspective***. Carlisle Barracks, PA: Army War College, April 1997. 34p.

Abstract: The subject of Information Operations (IO), formerly called Information Warfare, is having a profound impact on the Department of Defense and the Armed Services because of the proliferation of information technologies throughout the Armed Services. Most literature on the subject will tell you that IO is the center piece for a larger Revolution in Military Affairs. Whether these technological innovations represent a revolution or not, is of little importance in the grand scheme of things. But taking maximum advantage of their potential is. Utilization of these technologies is not without considerable risk. This paper examines where we got started with incorporating high technology into intelligence, weapons, and command, control, communications and computer systems, assess where we are and where we are going, discuss the associated vulnerabilities and what we are doing to protect against them.

ACCESSION NUMBER: ADA327427

http://handle.dtic.mil/100.2/ADA327427

Blackington, Robert E. ***Air Force Information Operations (IO) Doctrine: Consistent with Joint IO Doctrine.*** Maxwell AFB, AL: Air University, Air Command and Staff College, 2001. 60p.

Abstract: Is Air Force information operations (IO) doctrine consistent with joint IO doctrine as required by policy directives? To answer this question, this research paper analyzes the consistency between Air Force Doctrine Document (AFDD) 2-5, Information Operations, and Joint Pub (JP) 3-13, Joint Doctrine for Information Operations, in three principal areas: 1. The components of information superiority (IS) and definitions of the key terms IS, IO, and information warfare (IW). 2. Air Force addition of the terms counterinformation (CI), offensive counterinformation (OCI), and defensive counterinformation (DCI). 3. The capabilities and related activities used to carry out offensive and defensive IO.

ACCESSION NUMBER: ADA399888

http://handle.dtic.mil/100.2/ADA399888

Bohan, Patrick J. ***Joint Task Force - Information Operations (JTF-IO): Should One Exist?*** Newport, RI: Naval War College, 2005. 22p.

Abstract: Joint Publication 3-13, Joint Doctrine for Information Operations was published in 1998 to provide guidance on conducting joint information operations. This paper will demonstrate that this doctrine did not provide sufficient detail with respect to IO organization as evidenced by IO difficulties encountered during recent conflicts. In addition, current doctrine does not provide sufficient guidance on component IO tasking. Based on analysis of recent conflicts with respect to IO, creation of a Joint Task Force-Information Operations (JTF-IO) is warranted to provide component level control, direction and authority to conduct IO throughout the joint task force.

ACCESSION NUMBER: ADA463384

http://handle.dtic.mil/100.2/ADA463384

Bookard, Joe D. ***Defining the Information within Military Information Operations: Utilizing a Case Study of the Jammu and Kashmir Conflict.*** Fort Leavenworth, KS: Army Command and Staff College, 2006. 69p.

Abstract: The current operating environment requires the United States military to conduct military information operations throughout the conflict spectrum, during all phases, and across various military operations. A function of the U.S. military is to deter adversaries who oppose the will of the United States, and if unsuccessful, render them incapable of physical resistance, thus ultimately altering their behavior. In essence, the U.S. military wishes to alter tangible and intangible variables in any system to gain an advantage. As the U.S. military increases its reliance on information and its supporting infrastructures, the threat will continue to become more sophisticated, clandestine, and complex. Therefore, military commanders and their staffs should develop sophisticated approaches to describe, classify, and explain essential elements within the information environment, particularly when conducting counterinsurgency operations (COIN). The commander's analysis of the information environment is critical. It will be challenged by anonymous adversaries in their remote geographic locations using inexpensive "off the shelf" technology. Because of this threat, there is a significant demand for accurate and reliable information for mission planning and execution for combat operations forces. The research presented in this work examines the Indian government's response to counterinsurgency through the categories of information defined by the author. The author's definition of information focuses on how decision makers, mainly military commanders, assign value to information within, and extracted from, the information environment. The definition is an attempt to add clarity to the broad meanings found in the FM and JP 3-13 doctrine for Information Operations. A bibliography of U.S. Government publications, books, monographs, reports, journal articles, and internet sites is included.

ACCESSION NUMBER: ADA449966

http://handle.dtic.mil/100.2/ADA449966

Borg, Charles M. ***Information Operations: Is the Army Doing Enough?*** Carlisle Barracks, PA: Army War College, 2001. 51p.

Abstract: For ten years the Department of Defense (DOD) and the Army have addressed information operations. Over the centuries militaries have conducted operations we today call information operations. In many respects the United States is the most prolific user of information operations while simultaneously it is most susceptible to them. For the U.S. to remain a world superpower and to ensure national security it must be preeminent in information operations. The Army, as a leader in information operations and a significant member of the national security establishment, must continue to improve its information operations capabilities. The Army's execution of information operations must and will tremendously reduce the potential for the United States to be strategically disadvantaged and should contribute significantly to its strategic advantage. United States Armed Forces will conduct operations under conditions of information superiority. Historically, the Army has conducted operations that today are considered information operations. This paper asks the question, is the Army doing enough to ensure its necessary and appropriate contribution in information operations? It provides background on DOD And Army information operations development and identifies shortfalls in current Army doctrine and training. The discussion ends with recommendations for improvements to the shortfalls identified.

ACCESSION NUMBER: ADA389747
http://handle.dtic.mil/100.2/ADA389747

Bortree, James R. ***Information Operations During the Malayan Emergency.*** *Monterey*, CA: Naval Postgraduate School, 2006. 79p.

Abstract: Today, Information Operations (IO) is an area of emerging importance in military science. IO however is not new. Many of the elements of IO have existed for hundreds, and in the case of specific elements like military deception (MILDEC), for thousands of years. IO becomes more important in dealing with the conflicts we face today, particularly as modern wars transition away from the large force on force encounters of the past. This thesis focuses on the specific British IO lessons learned during the Malayan Emergency. The thesis will also examine the IO implications of British organizational and cultural adaptation to counter the insurgents. Finally, it will also examine the most recent list of relevant Joint Doctrine, which drives how the individual services train, equip and resource forces for counter insurgency.

ACCESSION NUMBER: ADA451360
http://handle.dtic.mil/100.2/ADA451360
http://bosun.nps.edu/uhtbin/hyperion-image.exe/06Jun%5FBortree.pdf

Bouchard, Ronald M. ***Information Operations in Iraq***. Carlisle Barracks, PA: Army War College, April 1999. 48p.

Abstract: The United States effectively used information operations prior and during the Gulf War. In the wake of the U.S. led coalition victory, Iraq developed an asymmetrical approach to defeating any future coalition effort. Iraq's pattern of behavior demonstrated a growing mastery in perception management. Iraq's effective use of the media squashed U.S. efforts to establish a coalition response to Iraq's non-compliance with the UNSCOM inspections in early 1998. The successful use of information operations by Iraq in early 1998 shows how a small and unsophisticated desert country mastered the use of information operations. Taking from the lessons of trial and error an inexperienced Iraq effectively used asymmetric actions by using the media to influence international opinion and U.S. policy. This paper addresses the media, public opinion and policy prior to, during, and after the Gulf War.

ACCESSION NUMBER: ADA363160
http://handle.dtic.mil/100.2/ADA363160

Breazile, Gregory T. ***Defensive Information Operations in Support of the Marine Air Ground Task Force.*** Fort Leavenworth, KS: Army Command and Staff College, 2002. 113p.

Abstract: Currently the Marine Corps has no doctrine for information operations (IO). The Marine Corps Doctrine Division has published an IO concept paper from which to guide the development of IO doctrine. In joint and other service doctrine, IO is defined in both as an offensive and defensive capability. This thesis only discusses defensive IO (DIO) and will attempt to provide the reader with insight into how the MAGTF could conduct DIO. A USMC concept paper on IO, joint IO doctrine, and sister service IO doctrine were used to provide an understanding of how IO and DIO are defined by each. Additionally, analysis of the DIO threat and an overview of current MAGTF capabilities to conduct each of element of DIO (information assurance, physical security, operational security, counterintelligence, counterpropaganda, counterdeception, and electronic warfare) is provided. The thesis also analyzes historical examples of each DIO element to demonstrate relevance of each to MAGTF operations. Conclusions and recommendations are provided for each DIO element. This thesis demonstrates the need for DIO in support of the MAGTF and how the MAGTF should incorporate DIO into their service IO doctrine.

ACCESSION NUMBER: ADA406491
http://handle.dtic.mil/100.2/ADA406491

Brock, Mark E. ***How to Organize the Headquarters for Information Operations at the Brigade and Division.*** Fort Leavenworth, KS: Army Command and General Staff College, 2005. 82p.

Abstract: As the Army transforms into a modular force, the issue of information operations is a topic for leaders at all levels. A particular issue is how to organize the unit staff to plan, prepare, and execute information operations. Currently, units at the brigade and division level are trying various methods of incorporating staff officers and noncommissioned officers into the planning process for information operations. Some units are approaching the problem of integrating information operations into operations with the use of an Effects Coordination Cell (ECC). Other units have an Information Operations Working Group (IOWG) and a Fires Cell. The author asks the following question: what are the benefits of the ECC methodology as opposed to the separate IOWG and Fires Cell? The study attempts to determine which is the more efficient method, what is gained, and whether the process should be standard across the Army. Using Army doctrine and military journals, the author studied information operations planning and its implications for brigade and division headquarters. Taking into consideration available resources, the commander's intent, and numerous other factors leads to the conclusion that the ECC is the best way for these headquarters to organize.

ACCESSION NUMBER: ADA436501

http://handle.dtic.mil/100.2/ADA436501

Bromley, Joseph M. ***Evaluation of the Littoral Combat Ship (LCS) and SPARTAN SCOUT as Information Operations (IO) Assets.*** Monterey, CA: Naval Postgraduate School, 2005. 63p.

Abstract: This thesis will address the planned configuration of Lockheed Martin's Flight Zero, Module Spiral Alpha Littoral Combat Ship (LCS) and the ongoing development of the SPARTAN SCOUT, one of the Navy's Unmanned Surface Vessels (USV). Technology currently available as well as developmental technologies will be recommended for implementation in order to make the LCS and SCOUT assets to Information Operations (IO) objectives. Specific technology will include Outboard, TARBS, HPM, Loudspeakers, LRAD and Air Magnet. This thesis will include an evaluation of the current policy for authorizing Information Operations missions, specifically in the areas of Psychological Operations (PSYOP) and Electronic Warfare (EW).

ACCESSION NUMBER: ADA432431

http://handle.dtic.mil/100.2/ADA432431

http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Mar%5FBromley.pdf

Brock, Mark E. ***How to Organize the Headquarters for Information Operations at the Brigade and Division.*** Fort Leavenworth, KS: Army Command and Staff College, 2005. 82p.

Abstract: As the Army transforms into a modular force, the issue of information operations is a topic for leaders at all levels. A particular issue is how to organize the unit staff to plan, prepare, and execute information operations. Currently, units at the brigade and division level are trying various methods of incorporating staff officers and noncommissioned officers into the planning process for information operations. Some units are approaching the problem of integrating information operations into operations with the use of an Effects Coordination Cell (ECC). Other units have an Information Operations Working Group (IOWG) and a Fires Cell. The author asks the following question: what are the benefits of the ECC methodology as opposed to the separate IOWG and Fires Cell? The study attempts to determine which is the more efficient method, what is gained, and whether the process should be standard across the Army. Using Army doctrine and military journals, the author studied information operations planning and its implications for brigade and division headquarters. Taking into consideration available resources, the commander's intent, and numerous other factors leads to the conclusion that the ECC is the best way for these headquarters to organize.

ACCESSION NUMBER: ADA436501

http://handle.dtic.mil/100.2/ADA436501

Brown, Bill R., et al. ***Cognitive Requirements for Information Operations Training (CRIOT)***. Lawton, OK: Advancia Corporation, June 1999. 250p.

Abstract: The advent of battlefield digitization increases the work trainers for live force-on-force exercises must do to control exercises and provide feedback to units, and it will pull trainers at platoon and company level out of the tactical information loop. The goal of this study was to describe instrumentation capabilities with the potential for reducing workloads and pulling trainers back into the information loop for exercises at the Army's maneuver combat training centers (CTCs) and at home stations. This study documents the experiences of approximately seventy of the National Training Center (NTC) observer/controllers (OCs) and analysts that participated in the training of the Army's first digitized brigade during the Force XXI Army warfighting Experiment (AWE). To gain a better understanding of what is required to support digital training, the study team reviewed emerging tactical doctrine from platoon through battalion task force level to develop a sample of potential digital training points and then designed displays that would help a trainer monitor unit performance with respect to these points. The team then defined the capabilities a workstation would need to create these displays. This report describes, defends and illustrates twenty workstation capabilities that support exercise control and feedback for digitized units.

REPORT NUMBER: 1176-0001AF
ACCESSION NUMBER: ADA365483
http://handle.dtic.mil/100.2/ADA365483

Brown, Michael H. ***Employing Information Operations at the Marine Expeditionary Unit Level in the Sixth Fleet Area of Responsibility.*** Fort Leavenworth, KS: Army Command and Staff College, 2000. 60p.

Abstract: Information operations (IO) are defined as actions taken to affect adversary information and information systems while defending one's own information and information systems. Eased upon this definition, at the tactical level, the focus of IO is on affecting an adversary's information and information systems related to command and control, intelligence, logistics, maneuver, and firepower as they relate to the conduct of military operations while protecting our own capabilities. Military activities at the tactical level will often bear a resemblance to traditional operations with the 10 dimension being the effect these activities have at the operational level. The significance of this IO capability for a Marine Air-Ground Task Force (MAGTF) commander, specifically within the Marine Expeditionary Unit (Special Operations Capable) (MEU(SOC)), is important because it provides that commander with another way of effecting an opponent through direct or indirect means. Currently the Marine Corps does not possess the capability to perform IO at the MEU(SOC) level. The purpose of this monograph is to explore how the Marine Corps intends to employ offensive IO within the Sixth Fleet area of responsibility (AOR). The United States Marine Corps has maintained an active presence within the Sixth Fleet's AOR (Mediterranean Sea) since the end of the second World War. The MEU(SOC) is uniquely task organized, equipped, and trained to meet complex missions ranging from Noncombatant Evacuation Operations to amphibious raids. These missions would be enhanced once the Marine Corps develops the capability to employ IO at the MEU(SOC) level. The Marine Corps intends to develop this IO force for use within each of the MAGTFs (MEF, MEE, and MEU). The projected capabilities of this IO team would be to conduct limited offensive and defensive IO for the MEU commander.

ACCESSION NUMBER: ADA395006
http://handle.dtic.mil/100.2/ADA395006

Brumfiel, Timothy A., Sr. ***Information Operations Capability for the Armored and Infantry Brigade.*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2004. 85p.

Abstract: Presently, no organic information operations (IO) capability exists in the organization and structure of the armored and infantry brigade, so these brigades are unable to effectively plan, integrate, and coordinate IO activities into the brigade operations without assistance. As the Army transforms to a

more modular force that will rely heavily on the ability of brigades to conduct operations using assets normally associated with higher echelons or services, this capability becomes more relevant to the brigade to ensure success. This study analyzed field manuals, after-action reviews, lessons learned, and professional articles to determine the importance of IO to the brigade and to ascertain if a need existed for brigades to have their own ability to plan and coordinate IO activities. A survey was utilized to gain opinion from Army field grade officers attending the Army's Command and General Staff College (CGSC) to confirm the need for IO at brigade level. The study then provided a potential solution to the organizational structure that should be organic to the brigade to provide the needed IO capability. Based on the research conducted, evidence exists that there is a need for a trained, permanent IO staff member at the brigade level who can ensure that IO is fully planned, coordinated, and integrated into the brigade's missions and operations.

ACCESSION NUMBER: ADA428311

http://handle.dtic.mil/100.2/ADA428311

Buchholz, David R. ***Information Operations: Where Next?*** Newport, RI: Naval War College, 2005. 21p.

Abstract: This paper addresses the "ownership" of joint information operations (IO) by asking if U.S. Strategic Command (USSTRATCOM) is the right combatant commander to coordinate all Department of Defense (DoD) information operations. Doctrine already addresses the issue of combatant commander responsibility for ensuring that IO is planned and executed in the respective commands, but an IO vacuum exists with respect to standardized IO training and integration across the combatant commands. For this reason and others there is a compelling argument for the major responsibility for DoD information operations integration to fall under the control of U.S. Joint Forces Command (USJFCOM). The paper first explains how USSTRATCOM became the IO integrator for DoD IO. This is followed by the definition of joint IO as found in Joint Publication 3-13. The author then presents four historical examples of IO covering conflicts in four different geographic regions spanning 60 years. The examples include the use of IO during the Battle of Leyte Gulf in the Pacific theater, World War II; during Operation Desert Storm in Iraq; during Operation Noble Anvil in Kosovo, Serbia; and during Operation Uphold Democracy in Haiti. These examples highlight how IO, if successfully implemented, can be a force multiplier and mission enabler. They also shed light on the difficulties and consequences encountered if an IO strategy is not properly implemented. Finally, the command missions of USSTRATCOM and USJFCOM are analyzed to illustrate why USJFCOM is the command most suited to play the major role in the integration and projection of joint IO.

ACCESSION NUMBER: ADA464548

http://handle.dtic.mil/100.2/ADA464548

Buettner, Raymond. ***Information Operation/Information Warfare Modeling and Simulation.*** Monterey, CA: Institute for Joint Warfare Analysis, Naval Postgraduate School, [2000]. [46]p.

Abstract: Information Operations have always been a part of warfare. However, this aspect of warfare is having ever-greater importance as forces rely more and more on information as an enabler. Modern information systems make possible very rapid creation, distribution, and utilization of information. These same systems have vulnerabilities that can be exploited by enemy forces. Information force-on-force is important and complex. New tools and procedures are needed for this warfare arena. As these tools are developed, it will be necessary to provide education and training into their use. This project combines research to develop capabilities combined with concurrent development of instruction materials.

DKL D 208.14/2:NPS-IJWA-01-001 FEDDOCS

http://bosun.nps.edu/uhtbin/hyperion-image.exe/NPS-IJWA-01-001.pdf

http://handle.dtic.mil/100.2/ADA384028

Burnett Jr, Peter L. ***Information Operations.*** Carlisle Barracks, PA: Army War College, 2002. 37p.

Abstract: This SRP proposes designation of a single entity within the federal government to provide strategic guidance across the breadth of the nation's elements of power. It would coordinate and improve the security of the nation's critical information infrastructure, which is essential for the survival and prosperity of the United States. A review of the recent terrorist activities in the United States and the declaration of war against global terrorism revealed U.S. weakness in its ability to protect itself internally against terrorist activities. The United States found itself lacking in numerous areas. Area shortfalls include a lack of structure and policy and, in some cases, organizational structure that is focused on Homeland Defense. The U.S. also revealed an inability to protect its citizens, its physical infrastructures, the nation's economic structure, and critical information infrastructures. Numerous policies regarding domestic terrorist have been written and debated, but shelved. Older policy focused mostly on deterring terrorism and defeating terrorism abroad. On 11 September 2001, America witnessed terror firsthand in a well orchestrated attack that ripped and tore the economic and military fabric of its foundation. This event has prompted U.S. leaders to take a serious look internally at securing the liberty and prosperity of the nation's foundation. This study proposes ways and means of utilizing and protecting U.S. information operations in the war on terrorism.

ACCESSION NUMBER: ADA402019

http://handle.dtic.mil/100.2/ADA402019

Burton, Gerald V., Jr. ***Principles of Information Operations: A Recommended Addition to U.S. Army Doctrine.*** Fort Leavenworth, KS: Army Command and Staff College, 2003. 71p.

Abstract: It is imperative that Army doctrine fulfill its mandate to create common understanding across the force. This includes establishing a common basis for conducting IO across the spectrum of conflict. Army IO doctrine must provide commanders and their staffs the foundation necessary to effectively integrate IO into full spectrum operations. Without successful IO, achieving information superiority is unlikely. Without information superiority, the Army is at risk of failing to accomplish its assigned missions in the decisive manner that is expected and necessary. The soon to be released FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, represents a leap ahead in Army thinking about IO. It is particularly good at describing the IO threat and how the IO elements and related activities interact. It also presents numerous and detailed tactics, techniques and procedures for conducting (planning, preparing, executing and assessing IO). Still, this monograph asserts that FM 3-13 lacks a general, macro-level articulation of how IO elements are combined, so it needs to add a set of principles that guide commanders and staffs on how to combine the IO elements. This monograph seeks to discover whether or not existing U.S., Russian, and Chinese doctrine and theory can provide the sought after guidance on combining IO elements. The answer is yes. An analysis of all three nations writings on IO, and synthesis of the related ideas, shows they do offer potential solutions to the problem. These solutions are offered as recommended improvements to the ongoing Army IO doctrine debate. The monograph subscribes to the idea that IO is an integrating strategy, relating means to ends. Combining the elements is the essential part of this strategy, and must be guided by six principles. First, commanders and staffs must understand and leverage all three domIn making the case for these principles, the monograph covers several key areas.

ACCESSION NUMBER: ADA415801

http://handle.dtic.mil/100.2/ADA415801

Caldwell, Russell. ***Information Operations (IO) Organizational Design and Procedures***. Monterey, CA: Naval Postgraduate School, 2004. 179p.

Abstract: Multi National Force (MNF) operations recognize the existence of shared national interests in a specific geographic region. Furthermore, MNF operations seek to standardize some basic concepts and processes that will promote habits of cooperation, increased dialogue, and provide for baseline Coalition/Combined Task Force (CCTF) operational concepts. This thesis and its' recommendation for a Standard Operating Procedure (SOP) are aimed at improving interoperability and CCTF operational

readiness. The SOP will focus on the spectrum of Information Operations (10) with regards to Military Operations Other Than War (MOOTW) and Small Scale Contingencies (SSC) during MNF operations. First, existing doctrine and cases will be analyzed to develop a foundation for this study. This thesis will seek to identify the existing 10 procedures to be utilized during MNF operations. Next, exercise observations and lessons learned reviews serve as the basis for 10 SOP Annex development to support the MNF SOP.

ACCESSION NUMBER: ADA422171

http://handle.dtic.mil/100.2/ADA422171

http://bosun.nps.edu/uhtbin/hyperion-image.exe/04Mar%5FCaldwell.pdf

Carter, Rosemary M. ***Information Operations Coordination Cell-Necessary for Division Offensive Actions***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, December 1998. 67p.

Abstract: This monograph analyzes the need for a division Information Operations (IO) Coordination Cell during offensive military actions. The integrated concept team draft of FM 100-6, Information Operations: Tactics Techniques and Procedures, includes a division Information Operations Coordination Cell. The cell is responsible for integrating the components of Information Superiority (IS) to defeat the enemy's command, control, computers, communications, intelligence, surveillance and reconnaissance (C4ISR) while protecting friendly C4ISR. Their focus is the Information Operations segment of IS that includes operational security (OPSEC), psychological operations (PSYOP), military deception, electronic warfare (EW), physical destruction, computer network attack (CNA), public affairs (PA), and civil affairs (CA). The monograph restricts the topic to Offensive IO, or IO that attacks the enemy commander's ability to achieve his objectives. Also, the monograph limits the type of military action to offensive. The monograph focuses on offensive actions, the primary action within offensive operations, because that is what the Army is designed for; fighting and winning wars. The monograph analyzes the IO tasks using three supporting research processes. First, it determines that only five of the tasks are necessary for Offensive IO: PSYOP, military deception, EW, physical destruction, and CA. The monograph then analyzes current doctrine and the heavy division Army of Excellence Table of Organization and Equipment (TOE) to determine the division's capabilities to execute the Offensive 10 tasks. Finally, the monograph uses these capabilities and doctrine to determine if the current division staff has the necessary staff mechanisms to conduct the Offensive IO tasks.

ACCESSION NUMBER: ADA366192

http://handle.dtic.mil/100.2/ADA366192

Cave, William C. and Robert E. Wassmer. ***Defensive Information Operations Planning Tool***. Spring Lake, NJ: Prediction Systems, Inc., January 2000. 24p.

Abstract: This report describes the SBIR Phase 1 development and demonstration of a Defensive Information Operations Planning Tool (DIOPT) prototype, which will be used to minimize vulnerabilities and corresponding risks to operations, and interface with existing equipment security monitors and agents running autonomously or cooperatively. PSI's approach is based on computer technology that affords implementation of the planning tool using a laptop computer. Given operational plans for deploying an Information System (IS), a simulation of the IS can be constructed in the field using graphical icons depicting parameterized models tailored to specific scenarios to be represented. IS planners can construct the simulation by interconnecting icons representing IS nodes and links. Models of threats can be used to assess vulnerabilities of the system to various attacks. Planners can determine how the IS architecture can be improved to reduce vulnerabilities, and predetermine best courses of action to counter an attack. Once the DIOPT is completely implemented in Phase II, the laptop can be plugged into the actual system to capture real time data on IS architecture changes, malfunctions or suspected intrusions/attacks. This will cause alarms to summon the planner, to further investigate specified events automatically, and to aid in the rapid determination of the best courses of action to be taken.

ACCESSION NUMBER: ADA372867

http://handle.dtic.mil/100.2/ADA372867

Charlton, John W. ***War of Perceptions: Integrating in Formation Operations Into Peacekeeping Plans***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1998. 73p.

Abstract: U.S. military forces are conducting peace operations more frequently than ever before. Commanders in peace operations are faced with the dilemma of having to provide stability and security in an environment where the use of force is severely restricted. That problem, combined with potential adversaries that may not follow internationally recognized laws of warfare, could leave peace operations forces at a distinct disadvantage. Information operations provide a way for commanders of peace operations to combat this dilemma and meet mission objectives. This monograph analyzes how information operations (IO) can assist commanders and planners at the operational level of war in executing peace operations. It will answer the question, what role can IO play in a peace operation and how can planners at the operational level integrate information operations into their overall plan. In answering this research question, this monograph will first analyze peace operations as they relate to the physical, moral and cybernetic domains of conflict. Using examples from recent and ongoing peace operations, this analysis will demonstrate that commanders and staffs must consider more than the just the physical domain when planning a peace operation. The analysis will then shift to how the elements of operational design relate to peace operations. Finally, this monograph will address the specific requirements for integrating IO into the overall plan by analyzing staff organization requirements and IO functions in a peace operation.

ACCESSION NUMBER: ADA356951

http://handle.dtic.mil/100.2/ADA356951

Cheeseman, Curtis P. ***Information Operations - Hardnessing the Power***. Carlisle Barracks, PA: Army War College, 2002. 27p.

Abstract: Information Operations (10) 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 10 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 IC 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.

ACCESSION NUMBER: ADA401957

http://handle.dtic.mil/100.2/ADA401957

Clapp, Anthony J. ***Information Operations and Joint Vision 2020: Ready to Accept the Challenge.*** Newport, RI: Naval War College, 2002 24p.

Abstract: Ever increasing in importance to the Joint Force Commander (JFC) is the still evolving role of Information Operations (IO). Properly executed, IO will start during peacetime and play significant role in diffusing potential crisis situations. In times of crisis, IO will be a significant contributor to accomplishing the JFC's objectives and then will enable a smooth transition to a return to peace. However, it is currently not possible for the JFC to fully exploit all aspects of IO in order to gain and maintain an advantage over the adversary. Doctrinal shortcomings such as IO cell leadership and the IO organizational structure are the main obstacles preventing joint forces from reaping the benefits of fully integrated and synchronized IO. Joint Vision 2020 (JV 2020) poses a challenge to the operational commander by stating the pace of change in the information environment dictates that we explore broader information operations strategies and concepts. Joint forces should be prepared to accept this challenge, but must first change the way

they employ IO if they expect to achieve the JFC's objectives. Implementation of a Joint Forces Information Operations Component Commander (JFIOCC), led by the current Joint Psychological Operations Task Force Commander is the first step towards a synergistic approach to the employment of IO.

ACCESSION NUMBER: ADA400923

http://handle.dtic.mil/100.2/ADA400923

Costigan, James F. **Information Operations; Will We Be Ready for the Next Attack?** Carlisle Barracks, PA: Army War College, 2002.

Abstract: My thesis is that current doctrine establishes Information Operations in such a way as not to provide clarity on how we conduct operations today, but rather it is serving to muddy waters we're trying to navigate in. Our adversaries of the future will continue to focus along traditional and non-traditional means of attacking us. More emphasis will be placed on rogue and non-state players and their abilities to attack this nation. We can no longer afford to focus on traditional methods of conducting warfare. We must be prepared to fight and win both symmetrical and asymmetrical battles using both kinetic and non-kinetic means. The actions taken to protect and defend this country will require a significant cultural change on the part of the military and the nation. The defense of our nation is not just about protecting our shores against attack. It must include the defense and protection of our national infrastructure. We are not ensuring that the soldiers, sailors, airman, and marines, as well as civilians in the Department of Defense, are trained properly. Information technology changes rapidly. The warriors that will be required to use it, must have a skill set that is maintained accordingly. That doesn't happen today. Our strategic leaders must be looking 20 to 25 years down the road when implementing strategies for ensuring that such an infrastructure and all the value it possesses is still viable. They must have a vision that will guide our actions over the next quarter of a century. We must be open to change. Changes will need to be made in the way we look at Information Operations, the systems we use to fight our future wars, and the way we train our warriors of the future. If we fight this changing environment and the roles that come with it, we risk becoming a force that is irrelevant.

ACCESSION NUMBER: ADA401927

http://handle.dtic.mil/100.2/ADA401927

Cox, Joseph L. ***Information Operations in Operations Enduring Freedom and Iraqi Freedom -- What Went Wrong?*** Fort Leavenworth, KS: Army Command and Staff College, 2006. 134p.

Abstract: This monograph examines the integration of Information Operations (IO) during Operations Enduring Freedom (OEF) and Iraqi Freedom (OIF). As a rule, most commanders considered IO ineffective because IO was unable to respond to the complex environments of Afghanistan and Iraq. This monograph examines how the Army prepared commanders to integrate IO into operations in those two theaters of operations. Both theaters offer good examples of how some commanders integrated IO effectively, and how other commanders failed to integrate IO effectively. There are essentially three issues commanders must confront to integrate IO: doctrine, intelligence support to IO, and resourcing the IO efforts. First, Army doctrine does not provide commanders adequate guidance for integrating IO into their operations. Second, IO requires proper intelligence support to be effective, but intelligence doctrine and resourcing do not allow intelligence support to IO to be effective. Third, the Army has not resourced itself to conduct IO in an effective manner. As a result of these three issues with the Army's concept of IO, commanders do not understand how to integrate IO. This monograph will provide a series of recommendations that, if implemented, will help prepare commanders for the task of integrating IO. Those recommendations include doctrinal changes and modifications, organizational changes, training requirements, material resourcing requirements, leadership and education requirements, and personnel resourcing requirements. If implemented, these recommendations will make long-term changes to how the Army prepares commanders to integrate IO into their operations. The appendices discuss the relationship of Public Affairs to IO, provide an overview of IO organizational and equipment capabilities of the units identified in the main body of the monograph, and provide a more detailed breakdown of the various units that served in OEF and OIF.

ACCESSION NUMBER: ADA449922
http://handle.dtic.mil/100.2/ADA449922

Creekmore, Kevin. ***Battlespace Information Operations Simulation***. Huntsville, AL: Army Space and Missile Defense Command, January 1999. 7p.
Abstract: The Extended Air Defense Testbed (EADTB) is a medium to high fidelity constructive simulation that is used for theater-level operational planning and analysis of weapons systems. The EADTB was developed by the Testbed Product Office in the U.S. Army Space and Missile Defense Battlelab. It models all aspects of the battlefield to include sensors, communications, command and control (C2), munitions, and the environment. It offers a combination of scope, detail, and flexibility that is unique among simulations. The user is able to create the weapon systems, the C2 elements, threats, and the gameboard for the scenario to take place and then develop rulesets that determine the behavior of the systems in the course of the battle. One recent scenario built in EADTB was attlespace Information Operations Simulation (BIOS). The purpose of this experiment was to model dynamic Battle Management Command Control Communications and Intelligence, Surveillance and Reconnaissance (BMC4ISR) and the associated information management. The EADTB was able to provide visualization and analysis of decision processes, information flow and latency, and combat operations. It was also able to simulate the dynamic system response to changing conditions and assess the benefits of space assets.
ACCESSION NUMBER: ADA365027
http://handle.dtic.mil/100.2/ADA365027

Dougherty, Richard K. ***Organizational Structure for Inter-Agency Information Operations.*** Monterey, CA: Naval Postgraduate School, 2001. 221p.
Abstract: The purpose of this thesis is to stimulate a discussion toward developing an all-encompassing Inter-agency Information Operations organization. The authors define an environment and identify theories that point toward the necessity of integrating Information Operations (10) throughout the U.S. Government (USG). The authors explore the feasibility of establishing and empowering an inter-agency organization that will monitor, evaluate and enforce all aspects of IO. Early forms of IO and their deployment are depicted in the historical backdrop of World War II. Concepts of renown futurists identify the importance of the information Age and the essential process to maximize its' full potential. A correlation between the current national security strategy and the IO environment strongly suggests the need for innovation. An overview of the current IO environment and USG organizations reveals a technological move toward inter-agency IO. Both the art and science sides of IO are incorporated into a new organization. OrgCon 7.0 is used to analyze the proposed IO organizational structure, which provides specific recommendations and defines misfits that must be addressed. The authors conclude that further work is required in modeling the organization via alternate software and a more in depth look is required in the area of National Security IO. The authors provide the essential groundwork for further research.
ACCESSION NUMBER: ADA389648
http://handle.dtic.mil/100.2/ADA389648

Dovey, Thomas C., Jr. ***Conduct of Information Operations by a U.S. Army Division While Participating in a Stability Action***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advances Military Studies, December 1998. 55p.
Abstract: This monograph assesses the capability of a US Army Division conducting stability actions to plan and conduct Information Operations (IO) in accordance with the FM 100-6 coordinating draft, Information Operations: Tactics, Techniques and Procedures (FM 100-6CD) and Tactics, Techniques and Procedures (TTP) developed in recent stability actions. It identifies what IO tasks a US Army Division must be able to plan and execute in stability actions. It addresses what resources are required to conduct those IO tasks. The monograph then provides an assessment of the ability of the Division conducting stability actions to perform the required tasks. The monograph concludes that the Division is capable of planning and conducting information operations while conducting stability actions. However, this answer

assumes that the Division receives its habitual Psychological Operations (PSYOP) support element. The monograph brings out shortcomings in current IO doctrinal methods discusses new TTPs developed by divisions serving as TF Eagle in Bosnia Herzegovina and ends with recommendations for improving 10 doctrine and input for FM 100-6CD TTP CD.

ACCESSION NUMBER: ADA366180

http://handle.dtic.mil/100.2/ADA366180

Doyle, Kevin J. ***Information Operations: A Look at Emerging Army Doctrine and its Operational Implications***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1995. 56p.

Abstract: This monograph discusses how the Information Revolution is leading the Revolution in Military Affairs. Specifically, it examines the operational implications of the changing information environment, the army's doctrinal response (Information Operations), and the utility of Information Operations. The monograph examines the information environment and concludes that it gives nations and military forces unprecedented capabilities to acquire, manipulate, process and disseminate information. This implies that military forces will become much more efficient in maneuver, fires, and protection of forces. It also implies that information can be used as a separate element of combat power to attack directly the enemy's will to fight, to bolster US and coalition support for military operations, or to attack an enemy's information system to prevent him from doing the same. Because of this environment, information operations is emerging as a new area of warfare, and information is commonly considered as a fifth element of combat power. The monograph then examines the army's doctrine for Information Operations (IO). It finds that the army primarily treats IO as a force multiplier which enables ground forces to maneuver, fire, and protect the force more efficiently, rather than implementing IO as an element of combat power. The army doctrine does not detail the capabilities of the present force structure to support 10, and suggests creating no new force or task organization. The doctrine recommends an assistant staff officer in the operations staff section to synchronize IO, without detailing the responsibilities inherent. The doctrine credibly treats 10 as a supporting function which enables the force to develop the capability to execute simultaneous attack in depth.

ACCESSION NUMBER: ADA300222

http://handle.dtic.mil/100.2/ADA300222

Doyle, Michael P., et al. ***Value Function Approach to Information Operations MOE's: A Preliminary Study***. Wright-Patterson AFB, OH: Air Force Institute of Technology, Department of Operational Sciences, July 1997. 61p.

Abstract: A value focused thinking approach is applied to information operations. A preliminary value hierarchy for information operations is constructed by extracting the values of senior military leadership from existing doctrine. To identify these key values for information operations, applicable existing doctrine was reviewed and summarized. Additionally, hierarchical representations of the values represented within each reviewed doctrine are developed. A value hierarchy requires that supporting objectives be mutually exclusive and collectively exhaustive. Within this analysis, these requirements are enforced, in part, by developed definitions which serve as tests to maintain mutual exclusivity. An exhaustive set of supporting values is also guaranteed by identifying a spanning set of values that directly support the overall objective of information operations. This preliminary value hierarchy serves as the basis for continuing research. The implications for this research include the construction of a prescriptive model in which the effectiveness of current and future systems can be assessed on a common scale. Further, the effectiveness of developing technologies can be assessed and the value of these technologies determined with respect to the values of senior military leadership. With this, the value of holes in our suite of information warfare systems can also be assessed in terms of their effectiveness in fulfilling the values of military leadership.

REPORT NUMBER: CMSA-TR/97-04

ACCESSION NUMBER: ADA345554

http://handle.dtic.mil/100.2/ADA345554

Dragon, Randall A. ***Wielding the Cyber Sword: Exploiting the Power of Information Operations.*** Carlisle Barracks, PA: Army War College, 2001. 31p.

Abstract: *Information Operations (IO) are rapidly becoming a new Battlefield Operating System (BOS). Until the last 3-5 years, emphasis in applying the tenets of IO remained compartmented discretely within organizations at each level of war - strategic, operational, and tactical. Given the infusion of technology and the potential merger of those levels, information has become a currency for all operations across the spectrum of conflict. With the goal for IO to achieve Information Superiority, this study examines current IO doctrine and organization in light of expectations of the future battlefield and the transformed Army. The fundamental conclusion is that to develop into a viable contributor as a warfighting domain, IO should be formally recognized as a BOS and sub-divided to encompass two types of operations: influence/perception operations focused on the message; and network/cyber operations focused on the media. In the final analysis, current IO systems require radical modification with respect to doctrine, organization, leader development, and training.*

ACCESSION NUMBER: ADA390556

http://handle.dtic.mil/100.2/ADA390556

Duczynski, Guy. ***Making Information Operations Effects-Based: Begin with the End (-State) in Mind!*** Perth, South Australia: Edith Cowan University, 2005. 60p.

Abstract: *The literature on Effects Based Operations (EBO) continues to be dominated by theory, with limited evidence of (successful) practical application reported. This situation is entirely acceptable in the early formative stages of any new concept, as first hesitant steps are taken and the authority of a shared idea gradually develops. EBO is now a global phenomenon. The effects must have primacy in shaping the actions that are taken. EBO practitioners, particularly those within the information operations domain, need those hands-on executable actions that can be taken to solve problems in the real world. Furthermore, these executable actions can only be enabled through the possession of specific capabilities. The paper offers that a systems approach that includes a problem space, a solution space and a design space may bring the necessary totality to the subject, guarding against premature use of means that appear to fit well with the context a fixation with efficiency rather than effectiveness. The paper argues that an examination of the systemic interactions amongst factors may deepen planners or policy-makers understanding of why a region or area of interest behaves the way it does, before they attempt to change it. A method is detailed that couples effects statements and means and highlights capability requirements. A case study example is provided using North Korea.*

ACCESSION NUMBER: ADA472241

http://handle.dtic.mil/100.2/ADA472241

Duklis, Peter S., Jr. ***The Joint Reserve Component Virtual Information Operations Organization (JRVIO); Cyber Warriors Just a Click Away.*** Carlisle Barracks, PA: Army War College, 2002. 32p.

Abstract: *Informational power has now been coined as a national power along with political, economic and military powers. Moreover, Information Operations (IO) is a key stratagem to protect and facilitate our national interests across the full spectrum of engagement. The Department of Defense (DoD) incorporates information operations as part of all of its current plans, operations and exercises. Yet, there are very few organizations dedicated solely to IO. However, DoD conducted the Reserve Component Employment 2000-2005 (RCE-05) Study in which it was directed that a Joint Reserve Component Virtual Information Operations Organization (JRVIO) be established to support joint and inter-agency organizations. In this paper, I will determine what virtual means, how it will be used for IO, and how a joint reserve unit is structured and functions. Furthermore, I will make a recommendation on how and where this/these JRVIO(s) should be utilized to support overall DoD Information Operations and specifically, Joint Commands and inter-agency organizations.*

ACCESSION NUMBER: ADA404656

http://handle.dtic.mil/100.2/ADA404656

Earl, Robert S. and Norman E. Emery. ***Terrorist Approach to Information Operations.*** Monterey, CA: Naval Postgraduate School, 2003. 149p.

Abstract: This thesis provides insight into how terrorist organizations exploit the information environment to achieve their objectives. The study establishes an analytical IO framework, by integrating US military doctrine with a fundamental approach to IO theory. The framework proves useful in examining the IO tools terrorists have assembled and how they implement them to influence their target audiences. The thesis shows that terrorists are, indeed, naturally linked to the information environment by their nature and strategy. Generally speaking, all terrorists employ IO tactically to enhance their operations. However, many organizations have a profound understanding of the information environment and also have the ability to manipulate information to achieve their objectives. Since, terrorist organizations are militarily weaker than the states they face and cannot rely on physical attacks to accomplish their goals, they must adopt an information strategy to achieve their objectives. This thesis emphasizes three primary conclusions: first terrorist conduct violent attacks in the physical environment to enable operations in the information environment. Second, terrorist integrate offensive and defensive IO to survive and appear legitimate to potential supporters and to the state. Finally, terrorists intentionally target four different audiences: opposing, uncommitted, sympathetic, and active to influence their perceptions.

ACCESSION NUMBER: ADA417439

http://handle.dtic.mil/100.2/ADA417439

http://bosun.nps.edu/uhtbin/hyperion-image.exe/03Jun%5FEarl.pdf

Eassa, Charles N. ***The Friction of Joint Information Operations.*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2000. 51p.

Abstract: Joint Publication 3-13, Joint Doctrine for Information Operations was published in 1998 to provide clarity and guidance for conducting joint information operations. This paper seeks to answer if the doctrine proved sufficient at the Joint Task Force Level. Outlining information's role throughout the levels of war and the requirement for information at the JTF level, this paper uses the hierarchy established by previous keystone joint publications to determine if the joint information operations doctrine expanded on the established framework. During this process, the friction caused by the focus of Joint Publication 3-13 is contrasted against the hierarchical joint doctrine. Joint Publication 3-13 created a great deal of friction. The publication did not sufficiently clarify the role or the value of information across the spectrum of conflict. It did not link the national instrument of power called information to military information operations to provide unity of effort. There was no discussion expanding the fundamentals of operational art from the joint information operations perspective. Technically oriented, Joint Publication 3-13 did not provide guidance for JTF Commanders to include information operations in their intent statements, concept of operations, or commander's critical information requirements. These omissions contribute to the friction of integrating information operations into JTFs.

ACCESSION NUMBER: ADA381926

http://handle.dtic.mil/100.2/ADA381926

_____. ***US Armed Forces Information Operations - Is the Doctrine Adequate***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2000. 45p.

Abstract: Ultimately, all military operations function on information. This requires an active thought process to protect the needed information and information systems as well as to exploit adversaries' information requirements. The sister services have pursued approaches in developing and resourcing Information Operations based upon their tactical requirements. Outlining the joint and service doctrines, this monograph suggests that doctrine at the operational and strategic level is a collusion of service tactical doctrine and is too broad in its guidance. The doctrine does not specify responsibilities at the operational or strategic levels nor does it afford for synergy based on the services' Information Operations

doctrine. The study concludes that the doctrine represent a solid point of departure to continue the refinement and delineation of Information Operations at the operational and strategic levels.
ACCESSION NUMBER: ADA374690
http://handle.dtic.mil/100.2/ADA374690

Englert, Marvin A. ***Applying Advances in Information Operations to Peace Enforcement***. Newport, RI: Naval War College, 2001. 23p.
Abstract: The Armed Services of the United States are experimenting with concepts that use recent advances in information technologies to enhance its information operations. Two of these concepts are Network-Centric Warfare and Army Battle Command System being developed by the United States Navy and the United States Army, respectively. These concepts are being applied to enhance military operations in the combat environment. However, there is some question as to their usefulness in the Military Operations Other Than War (MOOTW) environment that the Armed services will continue to be involved in. This paper examines the applicability of these concepts to information operations in the MOOTW environment using the peace enforcement operation in Bosnia, Joint Endeavor/Joint Guard, as an example. It also examines the impact these developments may have on our allies, coalition partners, government and non-government organizations in this environment.
ACCESSION NUMBER: ADA392869
http://handle.dtic.mil/100.2/ADA392869

Evans, Alan T. ***Department of Defense and the Age of Information Operations***. Carlisle Barracks, PA: Army War College, May 1998. 33p.
Abstract: This paper explains the challenges and vulnerabilities the Nation and especially the military will face in the next century as our dependence on information systems and associated infrastructure continues to grow. It will highlight the results of the President's Commission on Critical Infrastructure Protection and discuss the steps necessary to protect the information systems upon which we have come to so heavily depend. It will highlight that without a comprehensive national policy in protecting information infrastructures poses a great risk to its military, commercial users and ultimately the Nation.
ACCESSION NUMBER: ADA345602
http://handle.dtic.mil/100.2/ADA345602

Feiring, Douglas I. ***Information Warfare...From the Sea. Integrating Information Operations and the Marine Corps Planning Process.*** Quantico, CA: Marine Corps Command and Staff College, 2001. 12p.
Abstract: Although the Marine Corps's current method of planning and employing Information Operations (IO) seeks to integrate its various elements, improvements must be made for this emerging concept to be a truly effective force multiplier.
ACCESSION NUMBER: ADA400017
http://handle.dtic.mil/100.2/ADA400017

Ferguson, Quill R. ***Information Operations: The Least Applied Element of U.S. National Power.*** Carlisle Barracks, PA: Army War College, 2004. 28p.
Abstract: Information operations, one of the four elements of U.S. national power, is supreme in defending the country against foreign or domestic adversaries and winning hearts and minds both at home and internationally. Following the terrorist attacks against the World Trade Center and the Pentagon on September 11, 2001, the majority of the world was outraged by the disregard for human life demonstrated by those who perpetrated the destruction. However, there also was strong animosity towards the United States throughout the Islamic World, particularly in the Middle East, that resulted in an acceptance of the act on the part of many Muslims. This paper examines the effectiveness of the U.S. Informational Element of National Power, compares it with those of U.S. adversaries, and determines what changes must occur to strengthen it. Finally, a recommendation is made on how the United States

can regain the lead in winning the hearts and minds of adversaries and potential adversaries around the world.

ACCESSION NUMBER: ADA424076

http://handle.dtic.mil/100.2/ADA424076

Ferriter, Michael. ***Information Operations: Training the Leaders***. Carlisle Barracks, PA: Army War College, April 1999. 24p.

Abstract: The purpose of this project is to determine if the Army's officer education and training systems adequately prepare our leaders to operate within, and to deploy, fight, and win in the Information Age. As we depart the industrial age and enter the Information Age the United States Military is undergoing a Revolution of Military Affairs (RMA). I undertook this project to exploit the opportunity to study this area. In this project I describe and define Information Operations as they are defined by our doctrine. I place IO with the context of the strategic environment, and the role of IO across the Range of Military operations and spectrum of conflict. I review the Army's plan to establish and integrate information operations within the Army. I describe how the Officer Personnel Management System XXI (OPMS XXI) restructured the officer corps along related branches and functional areas. I assess the professional military education system's current and future plans to address IO and offer recommendations believe will assist the effort.

ACCESSION NUMBER: ADA367956

http://handle.dtic.mil/100.2/ADA367956

Francis, Trisha. ***Requirements Analysis for the Development of Digital Library for the DoD Information Operations Center for Excellence (IOCFE).*** Monterey, CA: Naval Postgraduate School, 2006. 47p.

Abstract: In a memo from Paul Wolfowitz, Deputy Secretary of Defense, "The Naval Postgraduate School (NPS) is hereby designated the DoD Information Operations Center for Excellence. In that capacity, NPS shall facilitate development of Information Operations as a core military competency and innovation." Commander, US Strategic Command (USSTRATCOM) will serve as Operational Sponsor for the Center on behalf of the Combatant Commands. The Secretary of the Navy and Commander USSTRATCOM will develop a charter for the Center on Wolfowitz's approval, in coordination with the Under Secretaries of Defense for Policy and Intelligence, the Chairman of the Joint Chiefs of Staff, and other DoD officials as appropriate. The charter will address oversight and activities of the Center, including graduate education, research, research opportunities, and transformation. As a tool to enhance the IOCFE USSTRATCOM is looking into the development of a digital library which will specifically provide resources for the Information Operations Community. This thesis conducts a preliminary requirements analysis for the development of a digital library. Successful development of this digital library is expected to effectively enhance the operational areas of Information Operations and Information Warfare within the Department of Defense.

ACCESSION NUMBER: ADA456944

http://handle.dtic.mil/100.2/ADA456944

http://bosun.nps.edu/uhtbin/hyperion-image.exe/06Sep%5FFrancis.pdf

Freeman, Bryan R. ***The Role of Public Diplomacy, Public Affairs, and Psychological Operations in Strategic Information Operations***. Monterey, CA: Naval Postgraduate School, 2005. 77p.

Abstract: Organizing for and conducting effective public affairs, public diplomacy, and psychological operations in support of national security objectives is a complex endeavor. In many instances, the desired psychological effects are contingent upon the efficiency of the organization conducting the programs and the development and dissemination of appropriate messages and themes. At present, the U.S. Government's ability to influence on a global scale is deficient due to fragmented organizational structure and underdeveloped doctrine relating to strategic influence. Duplication of efforts, inconsistent themes, and the lack of a long-term, strategically focused, integrated information strategy have been inhibitors to American foreign policy success. Following the terrorist attacks on September 11th, the U.S.

Government and the American people have wondered why we have been unable to effectively influence the majority of the population in the Middle East. Since that time, the government has struggled with the question of how to both organize for and effectively conduct a strategic influence campaign in support of the Global War on Terror (GWOT). The United States' present capacity to conduct strategic influence in the Middle East is hindered by a dysfunctional organizational structure relative to strategic information operations and an institutional reluctance to recognize or value strategic influence as an effective instrument of statecraft. This thesis examines the three primary components of U.S. strategic influence: public diplomacy, public affairs, and psychological operations. Next is a look at various U.S. strategic information programs, their organizational structure, and the changes that have occurred in focus and policies from the beginning of the 20th century to the present. The final chapter examines public diplomacy, psychological operations, and public affairs as they relate to Operation Iraqi Freedom.

ACCESSION NUMBER: ADA435691

http://handle.dtic.mil/100.2/ADA435691

http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Jun%5FFreeman.pdf

Gaines, Robert J. ***Future Information Operations (IO) in the Military: Is It Time for an 'IO CINC.'*** Maxwell AFB, AL: Air Command and Staff College, 2000. 29p.

Abstract: *The world is growing. Obviously not in terms of geography, but rather in the 'information' dimension. Populations, economies, and individual opportunity are each growing at rates unprecedented in the human experience. With this growth, the worldwide lust for information makes it a most powerful and necessary commodity. The world of Information Operations is where this commodity is produced, guarded, and marketed. If the United States of America is to maintain Superpower status, we must be pre-eminent in our Information Operations capability and readiness. The Department of Defense is funneling significant resources to meet this challenge. The question is: Under what command and control hierarchy are these efforts best shepherded? The first step in this study was to review existing literature on this topic and glean the present 'as is' condition of national Information Operations policy, military vision, private sector concern, law, and ethics. From this foundation, important issues were revealed and analyzed within the contextual framework. This research indicates our national interest would be best served through establishing an Information Operations Unified Command. Commitment and investment at this level by the National Command Authority and Department of Defense is logical and necessary to shape, respond, and prepare for worldwide Information Operations, potential Information Warfare, and cyber-terrorism.*

ACCESSION NUMBER: ADA394089

http://handle.dtic.mil/100.2/ADA394089

Gallogly, Erin J. ***Nonlethal Information Operations Targeting Process: Duties, Responsibilities and Procedures***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, December 1998. 60p.

Abstract: *This monograph's purpose is twofold. First, it provides the Joint Task Force Commander procedures by which to integrate nonlethal information operations into the joint targeting process and recommends duties and responsibilities for staff officers to ensure they integrate information operations into plans and operations. Second, it offers information operations officers a single document from which to develop standing operating procedures and tactics, techniques, and procedures. Joint Publications 3-0, Doctrine for Joint Operations, and 3-09, Doctrine for Joint Fire Support, provide the doctrinal underpinnings for joint targeting. Additionally, Joint Publication 3-13, Joint Doctrine for Information Operations, provides doctrine and guidance for information operations targeting. Currently there is neither Army doctrine for information operations targeting nor tactics, techniques, and procedures on how to integrate information operations into the targeting process. This monograph attempts to fill this gap. The capabilities, limitations, and employment considerations are outlined for the nonlethal information operations capabilities and activities (i.e., civil affairs, electronic warfare, military deception, psychological operations, public affairs, and special information operations). Finally, the author makes several recommendations in the areas of personnel and organization, training and education, doctrine, and operations.*

ACCESSION NUMBER: ADA366242
http://handle.dtic.mil/100.2/ADA366242

Garrison, W. C. ***Information Operations and Counter-Propaganda: Making a Weapon of Public Affairs***. Carlisle Barracks, PA: Army War College, March 1999. 37p.
Abstract: The U.S. military operates in a global information environment and is subject to propaganda influence from both domestic and foreign media. Access to information and disinformation can now influence attitudes and behavior from the battlefield to the far reaches of the world. Biased information can readily undermine the will of the American people and the American soldier to Support military operations. This study examines the role of Public Affairs in information operations. It identifies the need for Public Affairs to change the objectives of its Public Information function. It concludes with recommendations for Military Public Affairs to engage in defined counter-propaganda activity.
ACCESSION NUMBER: ADA363892
http://handle.dtic.mil/100.2/ADA363892

Gaver, Donald P. and Patricia A. Jacobs. ***Analytical Models for Battlespace Information Operations (BAT-10) Part 1***. Monterey, CA: Naval Postgraduate School, February 1998. 54p.
Abstract: Modem warfare uses information gathering resources ('sensors') and C4ISR capabilities to detect, acquire, and identify targets for attack ('shooters'). This report provides analytical state space models that include the capabilities of the above functional elements in order to guide their appropriate balance; this includes attention to the effect of realistic errors, e.g. of target classification and battle damage assessment (BDA). The great sensitivity of strike effectiveness to BDA error is described in the text and illustrated in Figures 3.12-3.15.
REPORT NUMBER: NPS-OR-98-001
ACCESSION NUMBER: ADA341929
http://handle.dtic.mil/100.2/ADA341929

_____. ***Analytical Models for Battlespace Information Operations. (Bat-IO) Part 2.*** Monterey, CA: Naval Postgraduate School, Department of Operations Research. February 1999. 27p.
Abstract: Modern warfare uses information gathering resources ('sensors') and C4ISR capabilities to detect, acquire, and identify targets for attack ('shooters'). This report provides analytical state-space models that include the capabilities of the above functional elements in order to guide their appropriate balance; this includes attention to the effect of realistic errors, e.g., of target classification and battle damage assessment (BDA). Also, an analytic stochastic model that illustrates multiple attractor/steady states is presented.
REPORT NUMBER: NPS-OR-99-002
ACCESSION NUMBER: ADA361307
http://handle.dtic.mil/100.2/ADA361307

Glock, John R. ***'Operationalizing' Information Operations.*** Maxwell AFB, AL: Air Command and Staff College, 2000. 47p.
Abstract: All military operations utilize information operations (IO). The Joint Staff and Services have written doctrine on IO. The cornerstone documents of the Joint Staff and Services, all refer to IO. Information Superiority is a core competency of the United States Air Force. Yet, there is virtually nothing written on how one actually operationally employs IO in support of a Joint Force Commander. The purpose of this paper is to address the question: 'How, at the operational level, does one employ offensive counter information operations (OCIO)?' This researcher decomposed the problem of employing OCIO into constituent parts. This methodology revealed that successful employment of OCIO requires a

force application process similar to that used when employing traditional forms of military force (e.g., air power). One still needs to establish objectives, identify targets, recommend capabilities, apply these capabilities against specific targets and after applying them assess their level of success. Having established the requirements of a process for employing OCIO, this paper then analyzes what aspects of the current joint targeting process need modification, and how to modify them in order to apply that process to OCIO. OCIO can use the existing joint targeting process with only minor modifications. To enhance the OCIO targeting process there are seven recommendations. These are: creating IO Target Materials, developing IO critical elements, establishing IO target folders requirements, formulating joint IO weaponeering methodologies, integrating IO and non-IO planning efforts, ensuring adequate access to IO capabilities and refining terminology.

ACCESSION NUMBER: ADA394084

http://handle.dtic.mil/100.2/ADA394084

Goble, Jeffrey J. ***Combat Assessment of Non-Lethal Fires: The Applicability of Complex Modeling to Measure the Effectiveness of Information Operations.*** Fort Leavenworth, KS: Army Command and Staff College, 2002. 56p.

Abstract: Military forces conduct information operations against one of the most complex, adaptive systems the human mind. Linear thought processes, prevalent in the military, correspond to, and understand well, the linear mathematics that measure the effects of lethal fires. They do not lend themselves well to the thinking necessary for understanding the effects of non-lethal fires on the complex adaptive system of the human mind. While each of the capabilities of information operations (IO) has individual Measures of Effectiveness (MOE), the cumulative effects they achieve, once integrated and synchronized in IO, are not simply a sum of each of the capabilities MOE. Nevertheless, these non-lethal systems, synchronized in information operations, must have predictive effects in order for commanders to employ them with confidence. Therein lies the problem; comprehensive MOE for information operations do not exist.

ACCESSION NUMBER: ADA402626

http://handle.dtic.mil/100.2/ADA402626

Gottschalk, Frederick C. ***The Role of Special Forces in Information Operations.*** Fort Leavenworth, KS: Army Command and Staff College, 2000. 117p.

Abstract: This thesis examines the role of the Special Forces Group in Information Operations. It focuses on providing information to the Joint Task Force planner and the Special Forces unit leaders. It provides the Joint Forces Commander and planner an understanding of Special Forces unit's core capabilities, mission types and operational methods. It provides the Special Forces leader an understanding of what Information Operations are, and how his unit fits into the overall structure of an Information Operation. The thesis looks at four recent operations (Just Cause, Desert Storm, Noble Obelisk and Joint Guard) and Special Forces unit's missions during those operations. The missions are explained and cross-referenced with the elements of Information Operations (Operational Security, Military Deception, Psychological Operations, Electronic Warfare, Physical Destruction, Physical Security, Counterdeception, Counterpropaganda, Counterintelligence, Special Information Operations and Computer Network Attack) to demonstrate the potential role of Special Forces units in future Information Operations.

ACCESSION NUMBER: ADA383815

http://handle.dtic.mil/100.2/ADA383815

Gray, Jaime V., et al. ***Information Operations: A Research Aid Includes Coverage of Information Warfare, Information Assurance, and Infrastructure Protection***. Alexandria, VA: Institute for Defense Analyses, September 1997. 129p.

Abstract: The purpose of this paper is to provide an aid for researchers engaged in studying aspects of military Information Operations, including subelements of Information Warfare, Information Superiority, and Information Assurance. These topics are also associated with National Critical Infrastructure

Protection. The document contains an annotated bibliography of research material arranged by principal subject areas (e.g., Information Operations, Defensive Information Operations, National Policy, Technology) believed to be of most value to new analysts of this field. Also included are the results of interviews conducted with several nationally recognized experts in an attempt to elicit main themes and suggestions for improvement. This document can provide an excellent starting point for identifying issues and options, as well as applicable policy and implementation publications.

REPORT NUMBER: IDAD2082
ACCESSION NUMBER: ADA338452
http://handle.dtic.mil/100.2/ADA338452

Gray, James L., Jr. ***Planning Information Operations to Enable Assured Access***. Newport, RI: Naval War College, 2001. 21p.

Abstract: The end of the Cold War brought about an exponential increase in the quantity and quality of long-range precision weapons available to Third World countries. This trend is going to make it more and more risky for U.S. forces to project power against a country who possess these weapons. The solution to this problem is currently being called "Assured Access" and is a very complicated subject. Information Warfare (IW) offers the potential to help solve the assured access problem by minimizing risk to forces operating within weapons range of a hostile country. The problem is that current plans are not being revised to fully integrate IW with other warfare disciplines. One method to focus this effort is to analyze IW functions in terms of operational functions. This allows for the analysis of IW mission enablers and detractors. The logical follow through would then be to develop workarounds so that incorporating IW results in an overall more effective plan. This same analysis can be used by the tactical commander to evaluate changing situations and alternate courses of action. It is time to start integrated planning and to exercise this capability with the fleet.

ACCESSION NUMBER: ADA389506
http://handle.dtic.mil/100.2/ADA389506

Gregory, Thomas R. ***Educating Officers in Information Operations: Is the U.S. Army Moving in the Right Direction?*** Fort Leavenworth, KS: Army War College, 2003. 50p.

Abstract: Information Operations are becoming increasingly important in military operations. While many of the components that comprise Information Operations are not new the U.S. Army is attempting to better synchronize these components to increase their battlefield effects. To accomplish this aim the Army has produced new doctrine for Information Operations and even created a new career field for commissioned officers (FA3O) to address Information Operations. This study examines the doctrine that exists to support Information Operations as well as how Information Operations is being incorporated into the Army's Officer Education System. The study begins by describing a current military operation where Information Operations was the main effort. This case study selected was an operation conducted in Bosnia Herzegovina titled, "Operation Bosanova". The study next analyzes current and future U.S. Army doctrine for Information Operations. Next, the study addresses how Information Operations are taught as part of the current Officer Education System. The study concludes with a series of recommendations for how Information Operations should be taught as part of the Officer Education System. The conclusion of the study is that while sufficient doctrine currently exists within the U.S. Army to conduct Information Operations, there is an Army wide lack of any education in the discipline. While a concerted effort is being made to ensure that the Army has trained FA3O officers, no real training exists for the remainder of the officer corps to become educated in the fundamentals of Information Operations. It is this lack Information Operations education for all officers that is the biggest identified weakness of this study.

ACCESSION NUMBER: ADA419838
http://handle.dtic.mil/100.2/ADA419838

Griffith, James L. ***United States Air Force Information Operations Doctrine: Is It Relevant?*** Fort Leavenworth, KS: Army Command and Staff College, 2000. 121p.

Abstract: This study examines the relevancy of US Air Force (USAF) IO doctrine, organization and training to accomplishing the Air Force's missions. This study evaluates the strengths and weaknesses of USAF 10 doctrine as compared to joint doctrine and current thoughts being considered by civilian theorist and foreign nations. The discussion provides the background for answering the primary thesis research question: Is Air Force IO doctrine, organization and training relevant in today's IO environment? To adequately analyze the answer to this question, the author provides a definition of relevancy, and defines the elements that constitute the current IO environment. These definitions provide the framework upon which to evaluate the USAF's efforts in developing IO doctrine, training and organization. IO provide the edge our military needs to counter the threat of cyberwarfare, weapons of mass destruction and terrorism. The USAF must expand its capability to defend its information and information systems while simultaneously developing air power tools that contribute to the Joint Force Commander's theater IO objectives. Incorporating IO into USAF operations is the only way to maintain our edge in today's environment.

ACCESSION NUMBER: ADA383817

http://handle.dtic.mil/100.2/ADA383817

Hardy, Charles K. ***Information Operations as an Element of National Power: A Practitioners Perspective on Why the United States Can't Get It Right.*** Carlisle Barracks, PA: Army War College, 2005. 30p.

Abstract: Most observers are disturbed to note that the United States of America, the lone superpower and the largest democratic and economically successful country in the history of the world, cannot or will not apply the means required to achieve overwhelming success in Information Operations. In simplest terms, the US is failing to apply a marketing strategy to sell democracy. How often do senior leaders acknowledge that Information Operations is critical to the success of combating terrorism? Consistently it is stated that "winning the hearts and minds," "winning the war of ideas," or "combating an ideology" is key to victory. If these declarations are true, then why do most senior commanders consistently state "we are losing the Information Operations fight?" The purpose of this paper is to examine the US strategic national policies on Information Operations (IO). Additionally, if the US has a strategic plan in place ,is it understood and integral to all operational concepts throughout the force. The author will identify and explain why the US consistently fails to achieve success in implementation of IO and will make recommendations on how to apply this element of national power to achieve the national strategic ends.

ACCESSION NUMBER: ADA432386

http://handle.dtic.mil/100.2/ADA432386

Harris, Jr, David A. ***Information Operations as a Counter to US Air Dominance: A Rival's Perspective.*** Fort Leavenworth, KS: Army Command and Staff College, 2007. 63p.

Abstract: The purpose of this monograph is to answer the question of what lessons over the past ten years of US air operations have foreign militaries integrated into their doctrine and organizations to counter US air dominance. By examining the air campaigns in Kosovo, Afghanistan, and Iraq through the lens of Chinese and Russians analysts, information operations has been the key lesson learned to counter US air dominance. From this analysis, some broader conclusions were made concerning the conduct IO in peace-time, the confusion surrounding IO terminology, the challenges of identifying deception in the targeting and operational analysis process, and the integration of IO and air superiority objectives within a campaign.

ACCESSION NUMBER: ADA470650

http://handle.dtic.mil/100.2/ADA470650

Heickero, Roland. ***Some Thoughts on the Application of Military Theory to Information Operations and Network Centric Warfare.*** Stockholm, Sweden: Swedish Defence Research Agency, 2006 27p.

Abstract: The transformation into a world based on communication and information leads to Information Operations (IO) becoming more important than ever. Thus, there is a need to develop new methodologies for successful IO that take into account the change towards network-enabling warfare capabilities. In a network-centric warfare approach it is important to understand the opponents' network structure and communication system and how they use these resources. Equally important is to understand one's own network structure in terms of strengths and weaknesses. Every type of network has it own vulnerabilities in the form of vital nodes, links, and platforms, regardless of whether it is a communications, organizational, or biological network. If one understand one's own structure as well as that of one's opponents, the chances of effective IO increase greatly. A fruitful way forward is to use theories based on center of gravity (CoG) and critical vulnerabilities (CV). This paper first discusses the logic of networks in general terms and then considers different types of networks and their respective abilities to resist attacks of different kinds due to center of gravity and critical vulnerabilities. Twenty briefing charts summarize the presentation.

ACCESSION NUMBER: ADA461536

http://handle.dtic.mil/100.2/ADA461536

Hellquist, Ingvar. ***Information Operations - Demands of Increased Cooperation Within the Cabinet and Between the State and the Private Sector.*** Carlisle Barracks, PA: Army War College, 2003 29p.

Abstract: This paper presents a comparison of Swedish and U.S. perspectives on actions to reduce vulnerabilities in critical infrastructure when that infrastructure is attacked via Information Operations. It compares the U.S. and the Swedish definitions of Information Operations and offers an example of how Information Operations can be implemented. The paper stresses the need for increased cooperation among governments and increased awareness of a government's needs within the economic environment. With technological advancements occurring mostly in the private sector, no single actor is the owner of a critical information system. Yet information technology and globalization lead to the international arena and demand international cooperation. This paper suggests ways in which different actors (e.g., the Government, information system producers, suppliers of data and telecommunications equipment, financial institutions, insurance companies) can attain cooperation throughout a nation's critical systems. An area of special interest, because of their authority and collaboration in an asymmetric environment, is the role of police and military in protective Information Operations. The paper looks at the issues of global security, technological development, and economics as they affect Information Operations. The author stresses the need for developed forms of public-private cooperation and describes a way to organize traditional domestic responsibilities to keep pace with emerging information technology-related threats. The author also recommends new ways of handling crises and conflicts and enforcing sanctions in the international arena. Recommendations are provided for cross-sector security cooperation within the cabinet and between the State and private sector.

ACCESSION NUMBER: ADA414596

http://handle.dtic.mil/100.2/ADA414596

Hestad, Daniel R. ***A Discretionary-Mandatory Model as Applied to Network Centric Warfare and Information Operations.*** Monterey, CA: Naval Postgraduate School, 2001. 84p.

Abstract: The concepts of DoD information operations and network centric warfare are still in their infancy. In order to develop concepts, the right conceptual models need to be developed from which to design and implement these concepts. Information operations and network centric warfare are fundamentally based on trust decisions. However, the key to developing these concepts is for DoD to develop the organizational framework from which trust, inside and outside, of an organization may be

achieved and used to its advantage. In this thesis, an organizational model is submitted for review to be applied to DoD information systems and operational organizations.
ACCESSION NUMBER: ADA387764
http://handle.dtic.mil/100.2/ADA387764
http://bosun.nps.edu/uhtbin/hyperion-image.exe/01Mar_Hestad.pdf

Hill, Brian A. ***Can't We All Just Get Along? The Interagency Process at Work in Information Operations.*** Newport, RI: Naval War College, 2006. 22p.
Abstract: The United States military recently adopted an unprecedented strategy to meet the national military objectives of preventing conflict and surprise attacks. Preemption has taken on new meaning for the Department of Defense (DoD). The commander of Joint Task Force (JTF) Horn on Africa (HOA), Major General Timothy Ghormley, USMC, is leading 1,500 U.S. military personnel in Eastern Africa engaged in a battle without bullets. By attempting to stem the growth of radical Islamic militancy in East Africa, JTF-HOA aims to defeat Al Qaeda before kinetic weapons have to be fired.
ACCESSION NUMBER: ADA463536
http://handle.dtic.mil/100.2/ADA463536

Hollman, Ryan D. ***Descriptive Study of Information Operations and Information Warfare Awareness in the United States Air Force***. Wright-Patterson AFB, OH: Air Force Institute of Technology, School of Logistics and Acquisition Management. September 1998. 69p.
Abstract: Information has always been important in military affairs, conflicts, and wars. Information warfare is an important new concept that is emphasized by the significance of computer and information technology. The United States Air Force has educated and trained individuals in information warfare since recognizing the importance of information warfare in 1995. The Air Force Information Warfare Center and the information warfare squadron were also created to address information warfare concerns. Information warfare is important to the entire Air Force. How familiar are Air Force people generally in information warfare. This thesis addresses awareness of information warfare and information operations concepts. Despite the amount of focus, training, and education, it was unknown how aware individuals were concerning information warfare and information operations. This thesis surveyed eight hundred officers and enlisted personnel with a response rate of 214 to determine the baseline of information warfare awareness. Approximately sixty percent of the respondents indicated that they were aware of information warfare. Also, individuals who received information warfare training responded higher than individuals without training. This is the first study in information warfare and information operations awareness. Additional research is needed to determine how the awareness levels are changing and the effectiveness of the training.
ACCESSION NUMBER: ADA354317
http://handle.dtic.mil/100.2/ADA354317

Horner, Stephen C. ***Cryptography, Information Operations and the Industrial Base: A Policy Dilemma***. Carlisle Barracks, PA: Army War College, April 1997. 34p.
Abstract: The information age is in full swing and it is changing the face of national security. The explosive force of information technology places the Global Information Infrastructure, the worldwide industrial base and the various world governments in both mutually supporting and somewhat adversarial positions. The information infrastructure is rapidly becoming the lifeblood for the world's industry and a critical part of the national infrastructure around the world. Consequently, the emerging operational regime of information operations is playing a critical role in the protection of U.S. national security interests and exploitation of adversary systems associated with information systems. Cryptography, long a traditional government area of interest, is taking on increased importance in industry, not only for protection of sensitive data but as a worldwide product market itself. The U.S. government cryptography policy must balance the need for continued U.S. dominance in information technology and the government's legitimate need to access data. U.S. dominance requires increased access to world

markets for U.S. cryptography technology. Solution to this policy dilemma requires a team approach by U.S. government and industry to provide the best answer.
ACCESSION NUMBER: ADA326657
http://handle.dtic.mil/100.2/ADA326657

Issler, Gordon D. ***Space War Meets Info War: The Integration of Space and Information Operations.*** Maxwell AFB, AL: Air Command and Staff College, 2000. 19p.
Abstract: The thesis of this paper is that until current legal, political and technical constraints are overcome concerning the weaponization of space, space operations should focus on integrating into the information operations campaign with the goal of gaining and maintaining information superiority. This paper will describe Space Operations and Information Operations as defined by current and draft joint publications, and then discuss the integration of these two areas to produce a synergistic effect on the operational level battlefield.
ACCESSION NUMBER: ADA406586
http://handle.dtic.mil/100.2/ADA406586

Jones, Synthia S., Bernard Flowers and Karlton D. Johnson. ***To Wield Excalibur: Seeking Unity of Effort in Joint Information Operations.*** Norfolk, VA: Joint Forces Staff College, 2002.
Abstract: Throughout history, many authors have used European folklore as a medium to express complex ideas and clarify issues. Most known is the legend of King Arthur, a memorable story replete with rich allusions and profound metaphors. The Arthurian legend depicts Britain as a divided country: factional and disjointed with feudal entities fighting for control of the land. All seemed lost until the Lady of the Lake gave King Arthur the sword, Excalibur. Wielding this sword with vision, Arthur unified the people to bring order to a troubled land. There is a similar need for order leading to unity of effort in the realm of Joint information Operations (JIO).
ACCESSION NUMBER: ADA421636
http://handle.dtic.mil/100.2/ADA421636

Keim, Steven M. ***From Policies to Procedures: The Next Step in Information Operations***. Carlisle Barracks, PA: Army War College, May 1998. 48p.
Abstract: An effective information operations campaign depends on the successful integration of information operations elements and capabilities into the joint force commander's overall operation plan. Information operations planning must begin at the earliest stage of a joint force commander's peacetime campaign planning and must provide a basis for subsequent information operations in crisis and/or conflict. Information operations planning for a particular military operation can occur as part of the deliberate planning cycle or in response to a crisis; therefore, this paper addresses information operations planning requirements in relation to the deliberate and crisis action planning processes. It also discusses methods of planning, integrating and executing information operations and provides some tactics, techniques, and procedures in an effort to link information operations policy and doctrine to information operations execution.
ACCESSION NUMBER: ADA347140
http://handle.dtic.mil/100.2/ADA347140

Kirpekar, Ulhas. ***Information Operations in Pursuit of Terrorists.*** Monterey, CA: Naval Postgraduate School, 2007. 231p.
Abstract: The Global War on Terror is in its sixth year now and the battle with the Islamist terrorists is being fought both in the physical as well as the informational domain. This research examines the relationship between terrorism and information operations keeping in view Martin Libicki's notion of information warfare as a Mosaic of Forms. This research begins with the basics of terrorism and

information operations and proceeds to highlight the use of information operations by terrorist organizations and in particular its use by Al Qaeda. In order to compare the complete spectrum of information operations being conducted by United States-led forces in this Global War on Terror this research includes two detailed studies on the prosecution of information operations from the perspective of both the United States-led coalitions and the anti-coalition elements in Afghanistan and Iraq. The study concludes by highlighting the relevance of Libicki's constructs in the context of the Global War on Terror and proposes a macro strategy to pursue the Islamist terrorists in the information domain.

ACCESSIOJN NUMBER: ADA474087

http://handle.dtic.mil/100.2/ADA474087

http://bosun.nps.edu/uhtbin/hyperion-image.exe/07Sep%5FKirpekar.pdf

Kucukozyigit, Ali Can. ***Electronic Warfare (EW) Historical Perspectives and Its Relationship to Information Operations (IO)-Considerations for Turkey.*** Monterey, CA: Naval Postgraduate School, 2006. 149p.

Abstract: The purpose of this thesis is the exploration of the relationship and interaction between Electronic Warfare (EW) and Information Operations (IO) core, supporting and related competencies. Understanding the definitions of information and its value, information superiority, and the decision making cycle provides the foundation for the thesis. Investigation of the historical transformation of EW from the U.S. Civil War to the First Gulf War, and also examining how the concept of IO has developed and evolved contributes to this study by helping to comprehend the modern day interaction between EW and each IO competency separately. This interaction is constructed upon the guidance and standards provided by the latest U.S. Joint Chiefs of Staff Publication Joint Publication 3-13 Information Operations. This study concludes that the relationship between EW and IO is increasingly interactive and consists of two aspects: limiting and interfering, and reinforcing and supporting. Also, the relationship between EW and each IO competency is not consistent between the core and supporting competencies. In addition to these conclusions, this study expresses some considerations for EW and IO applications with respect to the unique environment and requirements of the Turkish Republic.

ACCESSION NUMBER: ADA457350

http://handle.dtic.mil/100.2/ADA457350

http://bosun.nps.edu/uhtbin/hyperion-image.exe/06Sep%5FKucukozyigit.pdf

La Perla, Philip A. ***Creating Information Knowledgeable Leaders Through Information Operations Education.*** Carlisle Barracks, PA: Army War College, April 1997. 51p.

Abstract: To be effective on tomorrow's battlefield, we must become masters of the 'infosphere.' The Army needs leaders who have a deep understanding of warfare in the context of the information age. This study defines the information operations (IO) conceptual knowledge required in senior leaders to be successful in warfare in the information age. Then it reviews the status of 10 education at USAWO. This review then leads to recommendations for changes to the course curriculum based on the curriculum of the School of Information Warfare and Strategy's two-year pilot program. These changes are the catalyst for transforming industrial-age thinkers into information knowledgeable leaders.

ACCESSION NUMBER: ADA326793

http://handle.dtic.mil/100.2/ADA326793

LaBruzzo, Jon-Paul R. ***Influencing Friends and Allies: Information Operations Doctrine and the Role of the Combatant Commander.*** Newport, RI: Naval War College, 2007. 23p.

Abstract: Joint Publication (JP) 3-13 states that "Information operations (IO) are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial [emphasis

added] human and automated decision making while protecting our own." While this definition addresses the full measure of joint efforts in effecting the mind of the enemy decision maker, it cordons off other potential recipients of IO-friends and allies of the United States. The term adversarial in the JP 3-13 definition of IO is limiting; IO has beneficial application in US efforts to influence states and peoples friendly or allied with the United States. Certainly, some aspects of IO are best reserved for unfriendly target audiences namely actions to disrupt, corrupt, and usurp. But if IO represents a panoply of capabilities that can be used to affect the enemy it also includes capabilities that can be used to influence friends. Therefore joint IO doctrine should be changed to include friends and allies of the United States as targeted audiences (IO-F/A). Furthermore the geographic COCOM has a role to play in IO focused on decision makers friendly to the United States through Humanitarian Assistance and Disaster Relief, the Theater Security Cooperation Plan, and Strategic Communications. This paper examines the COCOM's vital role in IO-F/A and justifies the need for JP 3-13 to be changed to reflect the importance of that role and information operations vis- -vis friends and allies of the United States.

ACCESSION NUMBER: ADA470830

http://handle.dtic.mil/100.2/ADA470830

Lane, Randall C. ***Information Operations: A Joint Perspective***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1998. 57p.

Abstract: This monograph examines the current Department of Defense approach to the integration of information operations on the future battlefield. Technology has become one of the driving factors as the military enters into the twenty first century. With regards to this focus, each separate military service is capitalizing on information technological advances but not with a joint focus or shared desired endstate. Information technology and systems are an integral part to the emerging field of information operations, but without the joint efforts of each service and a central controlling element the military applications of information operations will never meet their intended purpose. This monograph first explains what information warfare and operations are along with their military applications according to each service: the Army, Navy, Marines, and Air Force. Secondly, this paper looks at what the emerging joint doctrine states concerning the definition, employment and integration of information warfare on the future battlefield. This portion of the paper examines joint doctrine concerning the integration of information operations at the operational and strategic levels with examples of how information warfare was conducted in recent deployments in Somalia, Bosnia and the Gulf War. Thirdly, the paper analyzes the potential problems determined from comparing the different service approaches to information warfare as opposed to an integrated joint approach. Lastly, this paper explores the possible military need to create either a functional command responsible for the integration of joint informational warfare or simply maintaining the current C2 structure and limiting the focus to C2W for further integration of information operations training and doctrinal employment. The recommendations proposed in this monograph are centered on developing an integrated joint approach to the training, doctrine and employment of information.

ACCESSION NUMBER: ADA356947

http://handle.dtic.mil/100.2/ADA356947

Lawrence, Susan S. ***Effects of Information Operations on Nonlinear Force Structures***. Carlisle Barracks, PA: Army War College, March 1999. 41p.

Abstract: This paper will address the advent of information operations and its effect on how the military will operate in the future. The goal is to highlight the need to aggressively pursue the execution of information operations' strategy and doctrine. Wrapped in this is the requirement to fix responsibility, clarify terms and understanding of 10, and find creative ways of responding to this new order of business. This may mean a whole new way of thinking that may alter our force structure to be more responsive to a threat. This paper also introduces the theory of nonlinearity and its effect on information operations. Leadership, innovation, and flexibility of task organization are essential to the success in Army operations. Future force designers must look at each mission uniquely and apply the right size and type of forces to meet the threat. This means units deploying in non-traditional ways; thus, the challenge of providing smooth, reliable information operations.

ACCESSION NUMBER: ADA363159
http://handle.dtic.mil/100.2/ADA363159

Leney, Derek J. ***Improving Information Warfare Targeting: An IW Fires System.*** Newport, RI: Naval War College, Joint Military Operations Department, February 1995. 30p.

Abstract: Information Operations (IO) has grown in importance during recent conflicts. Yet some aspects of IO coordination and integration have fallen short of expectations. This has led to a desire by many in the IO community to better manage Information Warfare "fires" using the Joint Targeting Cycle as a rational process for their execution. However, current doctrine and joint organizations do not adequately provide for control of these fires. This paper addresses the conceptual challenges of Information Warfare (IW) targeting, including the differences between attacking "will" and attacking "capability." Recent lessons learned in Iraq and Kosovo highlight additional IO problems within the Joint Targeting Cycle. An IW Fires System is proposed to address these shortcomings, providing a formalized and connected organization for IW targeting and fire support.

ACCESSION NUMBER: ADA465003
http://handle.dtic.mil/100.2/ADA465003

Luiijf, H. A. M. ***Survey of Information Warfare, Information Operations and Information Assurance.*** The Hague, Netherlands: Fysisch en Elektronisch Laboratory, 1999. 92p.

Abstract: Research survey on the phenomena Information Warfare, Information Operations (Info Ops) and Information Assurance. History, development, definitions and developments in various countries around the globe. Appendix with list of abbreviations of terms in these fields.

ACCESSION NUMBER: ADA367670
http://handle.dtic.mil/100.2/ADA367670

MacKenzie, Scot D. ***Executing Joint Information Operations: Where Do We Go After Kosovo?*** Newport, RI: Naval War College, 2001. 22p.

Abstract: Operation Allied Force, the NATO air operation in Kosovo, was the first major operation where Information Operations (I0) was formally implemented, albeit with mixed results. Like many other aspects of this historic operation, I0 affects were prosecuted in piecemeal fashion and far too late to be effective. Alliance problems aside, the joint warfighting team raised many concerns for how I0 affects are integrated into joint and combined operations. While the I0 report card is bleak, it is important to examine what went wrong and take steps to improve I0 during future joint operations. We have far to go as a joint community until we see the full strategic benefit of I0, which doctrine suggests is to "affect adversary or potential adversary decision makers to the degree that they will cease actions that threaten U.S. national security interests." This paper proposes taking two concrete steps to elevate the importance of information by recognizing IO as a unique operational planning and execution function. At the core of my proposal is forming a permanent I0 cell, properly staffed, and led by senior leadership. This cell will develop the precursor for successfully executing I0: a theatre-wide I0 strategy that is fully coordinated with all non-DOD agencies in an AOR. My thesis is generated from the I0 lessons from Kosovo, namely: 1) Make sure people know what I0 is; 2) Start I0 very early in planning; 3) Have a adequately staffed I0 cell headed by senior staff officer; 4) Have an I0 strategy that is implemented during peace and crisis. Kosovo bears out one important point: Joint I0 is not ready for prime time.

ACCESSION NUMBER: ADA389521
http://handle.dtic.mil/100.2/ADA389521

Mackey, Randall L. ***Information Operations: Reassessing Doctrine and Organization.*** Carlisle Barracks PA: Army War College, 2003. 42p.

Abstract: Information operations will play a key role in pursuing information superiority as part of the Joint Vision 2020 goal of achieving full spectrum dominance. Despite the importance of information operations within the U.S. vision of future conflict, the U.S. military does not have a consistent and coherent understanding of information operations. Information operations mission areas are ill defined and what should be basic terminology is complex, full of nuances, and inconsistent. Organization within DoD to accomplish 10 missions is also less than optimal. In some cases different unrelated 10 missions are assigned to organizations in an effort to consolidate responsibility for 10. Yet in other instances closely related missions that should be centralized are assigned to different organizations. This paper examines the various mission areas under 10 as currently defined, proposes modifications, and presents a new taxonomy for 10 and 10 component mission areas. This paper also examines current 10 organizations within DoD and makes recommendations for realignment of 10 missions.

ACCESSION NUMBER: ADA413656

http://handle.dtic.mil/100.2/ADA413656

Mackin, Patrick B. ***Information Operations and the Global War on Terror: The Joint Force Commander's Fight for Hearts and Minds in the 21st Century***. Newport, RI: Naval War College, 2004. 27p.

Abstract: Information Operations offers the Joint Force Commander with an alternative to using traditional military force when objectives are abstract or intangible. General Charles Holland, United States Special Operations Command, identifies the Muslim population as the Center of Gravity in our current War on Terror. Information operations may be the tool necessary to target this Center of Gravity. The successful Australian Defense Force (ADF) experience with Information Operations in two recent conflicts offer the United States valuable strategies in fighting the Global War on Terror. Examining the ADF IC methods and techniques offer today's Joint Force Commander (JFC) with approaches worthy of consideration in a conflict that is religiously and ideologically charged. Analysis of current U.S. efforts in Afghanistan and Iraq are explored and recommendations are provided for consideration in the struggle to win the Hearts and Souls of the greater Muslim population.

ACCESSION NUMBER: ADA422766

http://handle.dtic.mil/100.2/ADA422766

Martin, William J. ***Information Pervades All Levels of War: A Study of Information Operations in Iraq.*** Maxwell AFB, AL: Air University Press, 2003. 21p.

Abstract: According to U.S. Joint Military Doctrine, the central hypothesis of IO is exploiting the enemy s information and information systems, while protecting one s own. (JP 3-13) IO is a concept as old as warfare itself, but has attracted more attention in recent years due to leaps in information technology. Global Positioning System, data links, computer networks, and even the media represent just a few facets of this glittering gem. IO is ubiquitous and applies across all phases and ranges of military operations, and pervades all levels of war & tactical, operational and strategic, making it a nation s single most powerful weapon. Although used extensively throughout the history of warfare, nowhere else has IO served a more extensive role than in than in U.S. military actions in Iraq.

ACCESSION NUMBER: ADA424992

http://handle.dtic.mil/100.2/ADA424992

Masterson, Michael J. ***NAIC Support to Information Operations.*** Wright-Patterson AFB, OH: National Air Intelligence Center, 2002. 34p.

Abstract: The purpose of this document is to provide NAIC Information Operations mission overview and demonstrate the Dynamic Information Operations Decision Environment (DIODE) production process.

ACCESSION NUMBER: ADA406442

http://handle.dtic.mil/100.2/ADA406442

McGovern, Jim. ***Information Operations. A USN Perspective.*** Washington, DC: Department of the Navy, 2002. 16p.
Abstract: These viewgraphs give a navy perspective on Information Operations.
ACCESSION NUMBER: ADA406362
http://handle.dtic.mil/100.2/ADA406362

McKeown, Wendell B. ***Information Operations: Countering the Asymmetric Threat to the United States***. Carlisle Barracks, PA: Army War College, April 1999. 40p.
Abstract: The United States is dependent on information. As we move into the 21st Century our reliance on information systems will only increase. The cornerstone of Joint Vision 2010 is information superiority. Every facet of future military operations will be critically linked to an aggregate cyber network that relies on critical national infrastructures to provide for information superiority. This system of systems is vital in performing both routine and crisis action military activities. Our dependence on this infrastructure places the United States in a highly vulnerable position to asymmetric attacks. This paper will examine the impact on our military if it were unable to effectively communicate and coordinate. It examines the vulnerabilities of the information infrastructure and argues that recent national policy changes will be effective in dealing with the threats to both civil and military operations.
ACCESSION NUMBER: ADA363692
http://handle.dtic.mil/100.2/ADA363692

McKiernan, Brian J. ***Information Operations Roadmap: One Right Turn and We're There.*** Carlisle Barracks, PA: Army War College, 2007. 12p.
Abstract: During Secretary Rumsfeld's tenure, the Department of Defense embarked on one of the most far-reaching transformations in the history of the United States military. This transformation is largely driven by the rapid advances in information technology and the belief that information is more critical now to military success and will become even more critical in the foreseeable future. The Department of Defense addressed this assumption by formulating the Information Operations Roadmap with the objective of making information operations a core capability of future forces and a core military competency. The goal of information operations is to gain information superiority -- the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting the enemy's ability to do the same. Achieving and sustaining a significant information advantage over the adversary remains problematic, particularly in asymmetric conflicts. This project assesses the Information Operations Roadmap by examining non-military applications of information technology in the Information Age, reviewing current doctrine and assessing information operations during recent United States military operations. This study provides recommended adjustments to the Information Operations Roadmap based on this analysis.
ACCESSION NUMBER: ADA469629
http://handle.dtic.mil/100.2/ADA469629

McLaughlin, Lawrence W. ***Organizing for Information Operations Within The Joint Task Force.*** Newport, RI: Naval War College, 2003. 21p.
Abstract: Information operations (IO) continue to rise in prominence as a force multiplier for the joint force. Joint doctrine defines information operations as a broad range of capabilities and related activities that include operations security, psychological operations, electronic warfare, physical attack/destruction and special information operations. Given the importance and scope of IO across the spectrum of conflict, it would be logical that a robust organizational structure would be prescribed to support the multiple functions of IO and ensure the necessary coordination required to implement a comprehensive 10 campaign. Unfortunately, this is not the case. Joint doctrine inadequately integrates IO into the Joint Task Force (JTF) organization to address the many aspects of IO. The current doctrinal organization for the

conduct of IO - the 10 cell - does not provide for unity of command or centralized planning necessary to support the commander's IO effort. A potential solution to this problem is to create a new organization within the JTF command and control structure modeled after the Joint Psychological Operation Task Force (JS0TF). This would greatly increase the ability of the Joint Force Commander to plan and execute a comprehensive IO campaign that is integrated with, and complementary to, the overall campaign plan.
ACCESSION NUMBER: ADA415438
http://handle.dtic.mil/100.2/ADA415438

Miller, Earl E. ***Army Transformation and Information Operations: The International Legal Implications.*** Carlisle Barracks, PA: Army War College, 2002. 35p,
Abstract: As many nations throughout the world have become entrenched in what has been described as the information revolution, many legal parameters of information operations remain uncertain. Information is fast becoming a strategic resource that permeates every facet of the U.S. National Military Strategy. The proliferation of information-based technologies will substantially transform the Army's doctrine as well as its structure. The evolution of the information environment has specific legal implications within the international community. This paper examines these challenges and proposes to establish a framework for the inevitable global debate over related legal issues.
ACCESSION NUMBER: ADA404415
http://handle.dtic.mil/100.2/ADA404415

Mills, Charles D. ***The Linkage of Joint Operational Fires, Information Operations and the Army: Does the Army Have Effective Feedback Mechanisms that Integrate Operational Fires (Physical Destruction) and Information Operations?*** Fort Leavenworth, KS: Army Command and General Staff College, 2004. 63p.
Abstract: The information revolution seems to hold a lot of promise to the U.S. economy and the U.S. military, but rigid bureaucratic hierarchies make it extremely difficult for effective integration of operational fires and information operations (IO). As one observes the transformation of the U.S. military and other traditional institutions, they have been ill prepared to meet new organizational challenges posed by nonhierarchical, amorphous, and networked opponents due to adapting unevenly to the information revolution. This monograph serves only to suggest that the U.S. military has adapted to the information revolution unevenly due to constraints by institutional inertia, service rivalries, and conservative thinking. Doctrine traditionally has emphasized centralized control of fires as the most efficient means of matching fires to capabilities, missions, and desired effects. In Objective Force (OF), due to the complexity and importance of integrating lethal and non-lethal fires and effects within IO, employing fires will require positioning delivery systems in a way that allows the ability to apply effects where they are needed. Additionally, as the concept of information warfare (IW) becomes more popular with certain circles of the U.S. defense establishment, it is imperative that the U.S. Army and the fires support community begin establishing effective feedback mechanisms at the operational level that effectively applies IO across all phases of an operation, throughout the range of military operations, and at every level of war.
ACCESSION NUMBER: ADA429751
http://handle.dtic.mil/100.2/ADA429751

Mitchell, Mark E. ***Strategic Leverage: Information Operations and Special Operations Forces***. Monterey, CA: Naval Postgraduate School, March 1999. 231p.
Abstract: Special Operations Forces (SOF) have assumed a unique and expanded role as a strategic asset of the United States. The conjunction of changing political and security environments and new technologies present both challenges and opportunities for SOF. Special Operations Forces provide the National Command Authority (NCA) a variety of unique capabilities and expanded options for achieving strategic goals at minimum costs. The recent drawdown has placed even more value on the capabilities and leverage provided by SOF. Additionally the rapid pace of technological change – the 'information revolution' - has opened the door to a potential 'Revolution in Military Affairs' (RMA). New approaches to warfare, like Information Operations (IO), are beginning to emerge from the RMA. Information operations,

like SOF, can also provide a means to leverage limited resources. At the strategic level, SOF can provide support for IO; at the tactical level, IO can support of special operations (SO). Each has distinct implications for SOF. In either case, the object of the supporting operation is to generate or expand a window of opportunity for the supported operation. Separately, both SO and IO can provide economy of force. Properly employed, this leverage is multiplied and offers a tremendous strategic asset.

ACCESSION NUMBER: ADA360007

http://handle.dtic.mil/100.2/ADA360007

http://bosun.nps.edu/uhtbin/hyperion-image.exe/99Mar_Mitchell.pdf

Molinari, Robert J. ***Winning the Minds in 'Hearts and Minds': A Systems Approach to Information Operations as Part of Counterinsurgency Warfare***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2005. 63p.

Abstract: Do Information Operations (IO) contribute to success in counterinsurgency campaigns? What IO measures of excellence exist to demonstrate achievement of success in counterinsurgencies? These questions currently challenge U.S. military forces deployed to Operation IRAQI FREEDOM. This monograph develops a systems framework to better analyze and understand the interactions of IO subsystems as part of counterinsurgency operations. In addition to developing an adaptive systems framework to understand the importance of IO as part of COIN, this document explains the importance of system's aims to identify centers of gravity and feedback loops through existing doctrinal typology of situation-specific considerations. Feedback loops are developed into measures of excellence that allow synchronization and synergy of IO subsystems to be translated through cultural barriers and adjusted as necessary to affect the perception management of all targeted audiences in a counterinsurgency campaign. The historical case study analysis of the Malayan counterinsurgency (1948-1960) is utilized to describe IO as part of COIN systems approach.

ACCESSION NUMBER: ADA436114

http://handle.dtic.mil/100.2/ADA436114

Moorman, John R. ***The Future Role of Information Operations in Operational Art.*** Newport, RI: Naval War College, 2002. 19p.

Abstract: This paper looks at the relationship between the rate of technology development and the role of information operations in the operational art. Computer processing power has doubled every two years since 1959 in accordance with Moore's Law, bringing with it a corresponding decrease in cost. Networking computers has exponentially increased the power of individual computers in accordance with Moore's Law. These technological phenomenon have produced the information age, where the ability to gather, process and exchange information is the source of power and wealth. The military is adapting to the information age, incorporating information systems in its infrastructure and exploring new warfighting concepts such as network centric warfare, that leverage the power of networks. The increasing integration of technology into weapons systems and operational concepts will increase the operational commanders capabilities and vulnerabilities. Without a corresponding increase in information operations capabilities and strategies, the best strategy can be defeated by successful destruction of information systems. Future operational commanders must understand the effects of increasing technological development and integration, and the increasing role and significance of information operations that corresponds with it.

ACCESSION NUMBER: ADA405639

http://handle.dtic.mil/100.2/ADA405639

Morthland, Samuel P. ***Information Operations: The Need for a National Strategy.*** Monterey, CA: Naval Postgraduate School, 2002. 71p.

Abstract: This thesis explores the hypothesis that a national information strategy would enhance military effectiveness and national security. Analysis of the role of information in conflict, a definition of what information is, and how it can be used to support military operations establishes the foundation for the

thesis. Perception management, system destruction, and information exploitation are identified as key elements of to an effective strategy. They are reflected in the 17 information operational capabilities in joint doctrine. Four categories were created to differentiate the IO capabilities along offense/defense and technological/cognitive lines. The current focus of IO in the U.S. is the technical/offensive IO category, with less attention being given to the conceptual/ cognitive category. This may be due to a lack of strategic IO planning. Therefore, a planning methodology is developed herein and used to analyze the Administration's response to the terrorist attacks on 9/11/2001. A detailed analysis of the IO capabilities used identified two shortcomings: the failure to identify all key audiences, and not considering all the IO capabilities available. The thesis recommends adopting the concepts of a National Information Strategy and the IO strategic planning methodology used in the study.

ACCESSION NUMBER: ADA405812

http://handle.dtic.mil/100.2/ADA405812

http://bosun.nps.edu/uhtbin/hyperion-image.exe/02Jun%5FMorthland.pdf

Murphy, Edward F., et al. ***Information Operations: Wisdom Warfare for 2025***. A research paper presented to Air Force 2025. Maxwell AFB, AL: Air University, Air War College, 1996. 72p.

Abstract: A robust information operations architecture can provide leaders dominant battlespace knowledge and tools for improved decision making. US armed forces in 2025 need an information operations system that generates products and services that are timely, reliable, relevant, and tailored to each user's needs. The products must come from systems that are secure, redundant, survivable, transportable, adaptable, deception resistant, capable of fusing vast amount of data, and capable of forecasting. The information operations architecture of 2025 this paper proposes consists of thousands of widely distributed nodes performing the full range of collection, data fusion, analysis, and command functions-all linked together through a robust networking system. Data will be collected, organized into usable information, analyzed and assimilated, and displayed in a form that enhances the military decision maker's understanding of the situation. The architecture will also apply modeling, simulation, and forecasting tools to help commanders make sound choices for employing military force. This architecture allows the United States (US) armed forces to conduct Wisdom Warfare. The system can be used by the commander in chief, unit commander, supervisor, or technician. Somewhere in the workplace, in a vehicle, or on the person there will be a link to the sensors, transmitters, receivers, storage devices, and transformation systems that will provide, in push or pull fashion, all the synthesized information needed to accomplish the mission or task. Information will be presented in a variety of forms selected by the user.

ACCESSION NUMBER: ADA333260

http://handle.dtic.mil/100.2/ADA333260

Myers, John M. ***Operational Command and Control for Information Operations.*** Newport, RI: Naval War College, 2006. 26p.

Abstract: Information Operations (IO) has been a topic of great debate. Much of the discussion has stemmed from the fact no individual commander owns or controls the entire discipline. There have been several reasons for the lack of ownership such as IO supports all warfare areas, its application is an all-hands effort and there have been too few capabilities to command. Over the years, models have been proposed on how to command and control the discipline. Current joint doctrine provides a framework that has IO embedded in the J-3 organization. The doctrine offers a representative IO cell that is led by a J-39 cell chief who resides below the directorate level of authority. Unfortunately current doctrine does not provide adequate guidance for commanding and controlling this discipline. As the demand for IO increases and new capabilities come online, IO needs to be commanded vice coordinated. The traditional component commanders-by-physical domain (e.g., air, land, sea) breaks down in the information age and a new construct to deal with IO and information as weapons should be considered. This paper suggests the responsibility for IO during normal operations should be assigned to a Theater Information Operations Command (TIOC) who is OPCON to the combatant commander. Once a requirement for a Joint Task Force (JTF) has been established, the TIOC is OPCON as the Joint Force Information Operations Component Commander (JFIOCC) to the Commander, JTF.

ACCESSION NUMBER: ADA463534
http://handle.dtic.mil/100.2/ADA463534

Nitzschke, Stephen G. ***Information Operations: A Conceptual Perspective for Staff Organization and Force Employment.*** Newport, RI: Naval War College, 2005. 25p.
Abstract: The Joint Force Commander (JFC) lacks an adequate information operations (IO) conceptual framework. Current definitions derived from various service perspectives have hampered his ability to effectively implement an IO strategy in an efficient manner. A different IO conceptual framework, when combined with appropriate definitions, will allow the JFC to more effectively and efficiently organize and employ forces to accomplish IO objectives. This paper suggests a different perspective that recognizes all military capabilities as potential contributors to an IO strategy, and recommends appropriate definitions to help redefine the traditional roles of the information operations and information warfare officers. The new conceptual framework improves effectiveness by allowing the JFC to employ any military activity or capability in an IO strategy specifically focused on the unique decision space of friendly and adversary forces. Efficiency is obtained through a staff organization that reflects this reality. The IO officer becomes a special advisor to the commanding officer, with expertise in integrating military actions and activities to shape the decision space. His staff is augmented based on JFC mission objectives and associated priorities. The information warfare (IW) officer is a warfare specialist capable of fighting in the information domain. He can function within an IO cell or support other battlespace activities as a member of the operations staff.
ACCESSION NUMBER; ADA463228
http://handle.dtic.mil/100.2/ADA463228

Nussio, Ricky J. ***Sherman and Nimitz: Executing Modern Information Operations.*** Fort Leavenworth, KS: Army Command and Staff College, 2001. 49p.
Abstract: Information Operations has become a controversial subject in the US Army. Whether due to ignorance of actual employment techniques or reluctance to rely on non-tangible means, information operations are often only a check the block consideration for military planners. Emerging US Army doctrine emphasizes the use of information operations, stating that in some situations they can be decisive operations. This monograph examines two historical examples of modern warfare for the possible application of modern information operation (IO) principles. The information operations principles found in Student Text 3-0, Operations (destined to become Field Manual 3-0, Operations), are used as evaluation criteria to determine if modern principles were applied in past campaign plans. Significant and relevant issues from these case studies suggest there are a variety of employment methods for information operations. The purpose of this monograph is to increase the knowledge, understanding and applications of IO concepts through the examination of two case studies of modern warfare. These case studies demonstrate that IO principles have been part of modern US military art since the mid nineteenth century. In studying past conflicts a greater understanding can be gained by future military planners of the use of IO.
ACCESSION NUMBER: ADA390484
http://handle.dtic.mil/100.2/ADA390484

O'Brien, Gregory J. ***Information Operations and the Law of Perfidy.*** Newport, RI: Naval War College, 2001. 26p.
Abstract: The Department of Defense (DOD) Office of General Counsel concluded in an assessment of international law and information operations (IO) that using computer "morphing" techniques of an enemy leader to falsely broadcast that an armistice or cease-fire agreement had been signed would be a war crime under the law of perfidy. The law of perfidy prohibits IO that would invite the confidence of the enemy to lead him to believe that he is entitled to or obliged to accord, protection under the rules of international law applicable in armed conflict with the intent to betray that confidence. This standard is flexible, and deception and psychological operations being planned or executed now with IO methods will not be precluded by the General Counsel assessment described above.

ACCESSION NUMBER: ADA395074
http://handle.dtic.mil/100.2/ADA395074

O'Connell, Ed. ***Off the Trodden Path: Thinking Through the Military Exploration of the Information Domain***. Newport, RI: Naval War College, February 1997. 87p.
Abstract: Trends in today's security environment point to a changed information domain on the horizon--a cyberspace of increased density, interconnectivity and collaboration, where links and nodes have disappeared. As military planners, we are stuck somewhere between institutional skepticism reserved for new tricks, and the awe and wonder with which the rest of our society views this new frontier. Yet, insights provided by recent strategic information warfare exercises suggest the military is beginning to approach cyberspace from a new perspective--as a place like any other. These trends and early insights will have profound implications for how we project force into this changed cyberspace of tomorrow.
ACCESSION NUMBER: ADA327513
http://handle.dtic.mil/100.2/ADA327513

Osborne, William B., et al. ***Information Operations: A New War-Fighting Capability.*** A research paper presented to Air Force 2025. Maxwell AFB, AL: Air University, Air Command and Staff College, 1996. 76p.
Abstract: In its most basic form, commanders have always performed the functions of observe, orient, decide, and act (OODA loop) to prosecute military operations. As with Alexander the Great, history shows the military commander who best analyzes, decides, and controls the speed of the engagement prevails in nearly every conflict. To master the OODA loop, military leaders have pushed technology to obtain more information. Ironically, this situation now leads to the requirement to solve two fundamental challenges if the United States expects to maintain air and space dominance in 2025. First, the proliferation of unintegrated military war-fighting architectures gives the commander potentially conflicting perspectives of the battlespace. Second, the explosion of available information creates an environment of mental overload leading to flawed decision making. Failure to master these challenges critically weakens the military instrument of power. This paper presents a solution to these challenges by confronting commanders as they employ future airpower forces. Regarding the first challenge, the large number of specialized war-fighting architectures makes information integration supporting overall coordination and control more important and more difficult. Simultaneously, the speed and the range of modern weapons drastically reduces the time commanders have to integrate conflicting information and decide on a course of action.
ACCESSION NUMBER: ADA332471
http://handle.dtic.mil/100.2/ADA332471

Patschke, Gregory M. ***Information Operations And J-3: A Perfect Union***. Newport, RI: Naval War College, 2004. 33p.
Abstract: Information Operations (IO) during Operation Allied Force proved to be a failure. Since then, former IO planners and military war college students have focused on a lack of unity of command and unity of effort as primary catalysts for this failure. They proposed eliminating the IO cell concept and adopting either an IO task force or a specific IO functional component command. I disagree. Currently, we are experiencing an explosion of change within the IO community. Not only is the utility of IO being embraced among the different services, but also for the first time we have a unified command, U.S. Strategic Command, chartered with the responsibility of organizing and coordinating national-level IO for the regional combatant commands. These changes, along with painful lessons learned, debunk the notional IO task force and component concepts. The nature of IO is often misunderstood. IO is a strategy instead of a force. Thus, the IO organization under the Joint Task Force (JTF) J-3 offers the most effective way to integrate IO into the overall military plan. To plan and execute IO early, the combatant commander should stand up an Operational Planning Team (comprised of theater-specific IO planners from the combatant command as well as support organizations) until a JTF is activated. The JTF soul initially concentrate on shaping the battlespace through IO until sufficient forces are in theater. Finally,

joint IO doctrine fails to address how the IO cell should be internally organized. Properly manned disciplines within the different functions of influence operations, physical attack operations, network operations, and support will allow the JFC to execute a timely, deconlicted, and synergistic IO combat plan.

ACCESSION NUMBER: ADA422717

http://handle.dtic.mil/100.2/ADA422717

Patterson, LaWarren V. ***Information Operations and Asymmetric Warfare...Are We Ready?*** Carlisle Barracks, PA: Army War College, 2002. 30p.

Abstract: *Events of Sept 11th, 2001 have made clear one inescapable fact. Because of rapid advances in technology, particularly in the information arena, global communications now enable us to hear and see first hand issues, events and concerns from around the world. These in turn raise passions and compel people to rethink their own closely held beliefs, prejudices and hatreds, and in some cases morphing into actions such as espionage, sabotage or terrorism. Information Operations and future Asymmetric Warfare will have a major impact on the U.S. Army's ability to remain a viable warfighting entity as well as our simple survivability against future adversaries. Currently, the Army's Field Manual FM 100-6 (dated August 1996) is the most up-to-date guide on Information Operations available to the rank and file field soldier and leader. While at the same time, the Army's newest doctrinal publications, FM-I and FM 3-0, address the Army's future in terms of who we are, what we do, how we do it today, tomorrow, jointly and within the full spectrum of operations that is the asymmetric warfare environment. It is, therefore, tantamount that our policies and future Army vision ensure Information Operations as a tool against asymmetric warfare remain on the forefront of Army strategic planning.*

ACCESSION NUMBER: ADA402007

http://handle.dtic.mil/100.2/ADA402007

Patton, Gary S. ***Public Affairs and Information Operations: Integral or Incompatible***. Carlisle Barracks, PA: Army War College, 2000. 27p.

Abstract: *Today's complex, cyber-powered global information environment presents formidable challenges for the military. Facing the certainty of intrusive media and an overload of information, the military has elevated the importance of two related battlefield functions: public affairs (PA) and information operations (IO). PA serves as the military-media interface, tasked with the role of facilitating media coverage of military operations. In doing so, PA fulfills the obligation to keep the American people informed, and helps to establish the conditions that lead to confidence in America's military. 10 has a different purpose. It encompasses a wide range of offensive and defensive capabilities aimed at achieving information dominance over an adversary. Department of Defense joint doctrine identifies PA as a key related I0 activity. But the relationship between the two is problematic. On the one hand, PA deals with the public release of factual information. On the other hand, I0 may deal with false intentions, as an element of military deception or black propaganda activities. By association alone, actual or perceived I0 to manipulate public information could jeopardize the credibility of concurrent PA media relations, and potentially damage the credibility of the overall military mission. It will be the purpose of this study to further examine this 10-PA relationship under fire in Bosnia, as the initial I campaign there confronted multiple non-cooperative and IO-capable adversaries. Through this examination, the study will make a determination as to whether PA and I0 are integral or incompatible military functions. Additionally, the study will look at initial feedback on I0 and PA in more recent operations involving Kosovo. Based on these sets of experiences in the Balkans, the study will conclude with recommendations for a future direction for joint and service I0 and PA doctrine.*

ACCESSION NUMBER: ADA376340

http://handle.dtic.mil/100.2/ADA376340

Peifer, Kenneth V. ***An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy***. Wright-Patterson AFB, OH: Air Force Institute of Technology, December 1997. 178p.

Abstract: This study focused on determining if unclassified current and pending Air Force information warfare and information operations doctrine and policy is moving in the direction it should in terms of being complete, consistent and cohesive based on what has been mandated and studied about information warfare. A model of unclassified current and pending Air Force information warfare and information operations doctrine and policy was examined through criterion-based congruence analysis to make this determination. Investigative questions were developed in reference to the current state of unclassified Air Force information warfare and information operations doctrine and policy. Secondary data analysis was conducted along two paths. The hierarchical path included an examination of unclassified information warfare and information operations doctrine, policy and regulatory guidance. The academic path included an examination of studies and commentary on information warfare and information operations focusing on doctrine and policy. A model of unclassified current and pending Air Force information warfare and information operations doctrine and policy was developed. Then the model was analyzed for congruence in terms of completeness, consistency, and cohesiveness using the hierarchical and academic secondary data analysis as a diagnostic tool. The model was found to be partially incongruent in all three areas.

REPORT NUMBER: AFIT/GIR/LAS/97D-10
ACCESSION NUMBER: ADA340379
http://handle.dtic.mil/100.2/ADA340379

Phillips, Gary E. ***Information Operations - A New Tool for Peacekeeping.*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1997. 92p.

Abstract: This monograph discusses the application of information operations to improve the efficiency and effectiveness of peace missions ranging from peacekeeping to peace imposition. Using a variety of models and an examination of the components of information operations this monograph demonstrates the applicability of these operations to peace missions. Examples from recent history provide a backdrop for evaluating previous applications and investigating other potential uses of information operations to support peace missions. Based on the validation of applicability the possible increase in effectiveness and efficiency are postulated and potential resource savings evaluated. The monograph first examines the status of international relations as a result of the demise of the Soviet Union and the rise of information technology. The impact of these two earthshaking events have forever changed the face the world. As the nations of the world seek a new geometry of relationships without the Soviet Union the level of violence continues to rise. Without the unifying ideologies of the Cold War, many nations are seeking identity through ethnicity. This factor in conjunction with a freedom to act completely in promotion of national interests without the specter of a global nuclear war has led to a very unstable world. At the same time that United Nations pleads for resources to enforce peace on the new world disorder, nations are increasingly captured by domestic issues. The question becomes can we afford the expanding resources necessary to keep the peace and still answer domestic problems? The final sections of this monograph address the utility of information operations for peace missions. Information operations, the application of the continued advances in information technology, provides a tool to make peace affordable. Information operations allow cost effective solutions.

ACCESSION NUMBER: ADA331354
http://handle.dtic.mil/100.2/ADA331354

Pickle, James A. ***Developing Joint Information Operations Warriors.*** Carlisle Barracks, PA: Army War College, 2006. 20p.

Abstract: The Department of Defense (DoD) has recognized the importance of information operations (IO), particularly in light of continual technological improvements. Positive direction has been given by the Office of the Secretary of Defense and the Joint Staff, but the responsibility to organize, train, and equip

remains with the Services and allows for different interpretations. The goal of IO is to maintain information superiority and, thereby, decision superiority. While influence operations may aim at adversary perceptions, joint IO can't be left open for interpretation. Information is impacting the spectrum of conflict more than ever before. Information dominance has always been important, but the speed and methods at which it can be sent, analyzed, and acted upon is increasing exponentially. This project focuses on the need for a dedicated IO career force for the DoD to truly achieve information dominance. The analysis begins with a quick review of joint IO doctrine, Service approaches to IO, and IO personnel management. Next, IO education and training challenges are explored. Finally, recommendations to improve joint IO are broached in an effort to ensure DoD IO warriors can influence, disrupt, degrade, or deny an adversary's ability to make a coherent decision at a time of our choosing.

ACCESSION NUMBER: ADA448653

http://handle.dtic.mil/100.2/ADA448653

Rabena, William S. ***An Information Operations Approach to Counter Suicide Bomber Recruiting.*** Carlisle Barracks, PA: Army War College, 2006. 26p.

Abstract: *Information Operations (IO) is one of today's least understood, yet most common scapegoat for perceived Global War on Terrorism failures in Iraq. Despite the on-going efforts of strategists and commanders to leverage the media in an attempt to tell the "good news" successes in Iraq, news coverage continually gravitates towards acts of violence, especially suicide bombings. With or without media support, recent polls indicate that the Coalition has already won many of the "hearts and minds" of the Iraqi people. Yet, most of the success or failure of information operations is measured and stuck on telling only the "hearts and minds" story. The analysis from this study suggests that IO correctly shoulders blame for all the wrong reasons. More appropriately, IO is underutilized in what can be deemed a "kinetic-only" battle on the suicide bomber. This project proposes an information operations policy expansion in relatively unused supporting elements -- counterdeception and counterpropaganda. This will add a non-kinetic approach to the kinetic-centric fight on suicide bombers. The study will analyze how information operations, in the form of counterdeception and counterpropaganda, can target the recruiting base for suicide bombers. More specifically, the project explores the possible success that could be achieved when counterpropaganda and counterdeception address cognitive third order effects of those who are most influential to the potential suicide bomber's decision-making. This new approach targets the Sunni religious faction and the family. This departure from current information operations norms serves as a change to current strategy. The recommended strategy changes also are included in the study.*

ACCESSION NUMBER: ADA449231

http://handle.dtic.mil/100.2/ADA449231

Revilla, Arturo, et al. ***Information Operations Vulnerability/Survivability Assessment (IOVSA): Process Structure (Revision A).*** White Sands Missile Range, NM: Army Research Laboratory, 2003. 33p.

Abstract: *This document is a revision of the IOVSA methodology formalized in June 2000. The goal of this revised document will be the clarification of the work to be performed for each phase, the requirements, and the expected deliverables. Since this revision will be a living document, it will be updated as appropriate to include lessons learned. The intent of this revision is to facilitate the dialog between the U.S. Army Research Laboratory/Survivability Lethality Analysis Directorate (ARL/SLAD) and the decision-makers (program Executive Offices (PEOs), Program Managers (PMs), evaluators, contractors, etc.) for U.S. Army IT-based systems. As before, the IOVSA process will provide a structured methodology for assessing IT system/System of Systems (SoS) 10 susceptibilities and vulnerabilities. The process will provide flexibility that enables the analyst to customize it for the system/SoS under assessment. Additionally, the IOVSA results will provide critical information to system developers and decision-makers regarding the system's/SoS' 10 susceptibilities and vulnerabilities. Furthermore, enough information will be able to be extracted from the process to evaluate different countermeasure techniques and protection recommendations to determine their feasibility and cost/reward ratio.*

ACCESSION NUMBER: ADA415656

http://handle.dtic.mil/100.2/ADA415656

Richard, Charles A. ***Submarines and Information Operations***. Newport, RI: Naval War College, 2000. 22p.

Abstract: Information Operations and Information Warfare are efforts to exploit a resource that has long been essential for military operations: information. Information has become a new medium for conflict, a potent weapon and a lucrative target. The manned, mobile, combatant platform can conduct Information Operations. The nuclear-powered attack submarine, and its inherent virtues of stealth, mobility, endurance, and power intensity, gives unique opportunities for employment. As the U.S. Navy intends to embed IO capabilities in the fleet, sailors, not scholars, need to begin to examine and exploit the field.

ACCESSION NUMBER: ADA382092

http://handle.dtic.mil/100.2/ADA382092

Rogers, Carol J. ***The Functional Relationship Between Information Operations and Military Intelligence.*** Carlisle Barracks, PA: Army War College, 2001. 30p.

Abstract: Information operations are a new approach to managing and manipulating information. Through the ages, the possession of information has won wars, and the lack of it often led to defeat. This paper attempts to define the relationship between information and intelligence, and concludes that military intelligence professionals have the core competencies needed to be effective information operations officers. Focusing on a joint perspective, information operations is defined, using illustrations to clarify the multi-faceted information operations' missions. The impact of new technologies is examined, as it relates to the use of information as a tool for military leaders. The personnel requirements for IO are examined and compared to the core competencies of military intelligence. The findings indicate the redundancy and overlay of the primary personnel capabilities of information operations and military intelligence. The arguments lead to the conclusion that intelligence officers are best suited and qualified to perform the responsibilities of an information operations officer and to manage information operations.

ACCESSION NUMBER: ADA390557

http://handle.dtic.mil/100.2/ADA390557

Rogers, Stephen C. ***Improving Information Operations with a Military Cultural Analyst.*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2005. 50p.

Abstract: The concept and practice of using information as a tool in military operations to support political objectives has gained increased notoriety and emphasis within U.S. political and military arenas over the course of the last decade. Two particular publications of 2001, the Quadrennial Defense Review Report (QDR) and the United States Army Field Manual 3-0, Operations, highlight this fundamental shift in the growing importance of using information in warfare. Of particular importance, the 2001 QDR mandated that information operations be treated not merely as an enabling function, but as a core capability of future forces. Recent military operations conducted during Operation Iraqi Freedom (OIF), however, indicate that the application of this newly christened element of combat power has fallen well short of desired effectiveness. Without comprehensive changes in training, equipment distribution and personnel management, the Army will continue to struggle to employ information operations and fail to achieve the directives of the 2001 QDR. Fortunately, the Army has begun several studies in an effort to make the necessary changes to improve information operations. Yet one model that the Army has not yet studied is that of international marketing and advertising agencies. These firms have developed effective organizational structures, techniques, and procedures to share their ideas with people across a vast array of cultures, all with the intent of inducing a predetermined action. Gleaning the pertinent lessons from the international marketing model can help the Army empower tactical and operational commanders with the tools necessary to better understand the culture of a country, region, or area of operations. With this knowledge, these commanders could greatly improve the effectives of their information operations.

ACCESSION NUMBER: ADA436283

http://handle.dtic.mil/100.2/ADA436283

Romanych, Marc. ***Applying the Domains of Conflict to Information Operations.*** Alexandria, VA: JB Management, Inc., 2005.

Abstract: Military information operations (IO) are about information and its use as a means to fight an adversary. Fundamental to the use of information as a military capability, or perhaps even a weapon, is an understanding of the information environment and its utility to armed forces. However, several key concepts underpinning the conduct of military operations in the information environment are too abstract for practical application by operational and tactical level armed forces. As a result, commanders and staffs frequently relegate activities to affect the information environment to the realms of the esoteric or impractical. Recent work conducted by the Department of Defense's (DoD) Command and Control Research Program (CCRP) provides a useful basis for visualizing the structure and characteristics of the information environment. Of particular utility is a model that describes three domains of conflict the physical, information, and cognitive. Initially used to describe decision-making, this model, when combined with the two primary views of information- information-as-message and information-as-medium provides a useful framework for describing how information can be used to support military operations. To execute an information operation, a military force conducts activities to affect and protect information systems and networks in the physical domain. These actions are synchronized to affect information content, flow, and use in the information domain. The result is an information advantage that, in turn, generates effects to influence adversary and other organizations decision-making in the cognitive domain and subsequent actions in the physical domain. This paper explores the relevance of the CCRP's three-domain model to military IO. By applying the model to the doctrinal concepts of information environment, information superiority, and information operations, a view of IO emerges that field commands can use to convert doctrinal concepts into practical action.

ACCESSION NUMBER: ADA463046

http://handle.dtic.mil/100.2/ADA463046

Ruth, Brian G. and J.D. Eckart. ***Agent-Based Modeling of a Network-Centric Battle Team Operating Within an Information Operations Environment.*** Aberdeen Proving Ground, MD: Army Research Laboratory, 2003. 130p.

Abstract: A model developed to analyze the emergent behavior of a network-centric battle team undergoing hostile information operations (IO) stress events is presented. Networked battlefield platforms are modeled as mobile semiautonomous agents that operate within a cellular automata (CA) lattice. The CA form a discrete spatially extended dynamical system consisting of a parallel networked lattice of computational cells in two dimensions. A software framework that combines CA-based agents with a genetic algorithm was developed in order to explore the dynamics of two opposing but "coevolving" units of networked combat agents. Simulation results using two variants of the CA-based combat agent model, both of which include IO stress in the form of radio frequency communications jamming, are analyzed and discussed.

ACCESSION NUMBER: ADA411990

http://handle.dtic.mil/100.2/ADA411990

Saegert, Joseph A. ***Making IO Work: Exploring the Need for an Information Operations Command.*** Monterey, CA: Naval Postgraduate School, 2002. 113p.

Abstract: This thesis investigates the establishment of an Information Operations (IO) command and will stimulate further discussion and research of this issue. Concepts and definitions of Information Operations are presented to provide the reader a common framework of understanding upon which to base further discussion of IO. Current organizational structure, doctrine for execution of IO, and how IO supports national and military objectives are also presented and shortcomings examined. After consideration of several possible solutions a proposed structure for an IO command is presented and the feasibility of that structure discussed.

http://bosun.nps.edu/uhtbin/hyperion-image.exe/02Mar_Saegert.pdf

Sands, Thomas R. and Paul H. Issler. ***Special Operations Forces, Information Operations, and Airpower: Prescription for the Near 21st Century***. Monterey, CA: Naval Postgraduate School, December 1998. 121p.

Abstract: The Gulf War of 1990-1991 has been described as the pinnacle of second-wave warfare, characterized by massed field armies, maneuver formations based on the armored vehicle and airplane, second generation precision guided munitions (PGMs), and engagements involving thousands of soldiers, sailors, airmen, and marines. At the height of the conflict, over 500,000 United States (U.S.) servicemen were deployed in support of Operations DESERT SHIELD/DESERT STORM. The ensuing victory by U.S./Coalition forces and loss by Iraqi forces is one of the greatest lopsided outcomes in the history of warfare. Unfortunately, the demonstrated U.S. preeminence in conventional second-wave warfare may spell trouble for the 21st century. Potential adversaries will have taken note of our capabilities in this arena and will endeavor to develop methods and technologies that will negate our strengths either through asymmetric attack, innovation, or both. These actions will give rise to asymmetric warfare as the dominant paradigm. Combined application of special operations forces (SOF), information operations (IO), and airpower (AP) may produce synergistic effects that will permit smaller forces to effectively and efficiently counter our adversaries adopting asymmetric warfare. We employ a heuristic approach in conveying our vision of combined SOF, IO, and AP operations.

ACCESSION NUMBER: ADA360045

http://handle.dtic.mil/100.2/ADA360045

http://bosun.nps.edu/uhtbin/hyperion-image.exe/98Dec_Sands.pdf

Schutze, James T. ***Defensive Information Operations - An Interagency Process***. Carlisle Barracks, PA: Army War College, 2001. 33p.

Abstract: The United States military has long held the mission of protecting this country against foreign attack. One of the biggest threats facing the United States in the 21st century, however, is of a far different nature than that of a conventional armed attack. A cyber attack zeroing in on critical information or on the information systems which support critical national infrastructures could be launched from any corner of the globe, by a variety of potential state and non-state actors, and could be directed against military or civilian targets. Due to the quantity, complexity, and diverse ownership of this country's information systems and critical infrastructures, no single governmental or private agency can single-handedly provide an adequate defense. As a result, the nation's information and infrastructure protection effort requires governmental interagency and private sector cooperation. The Department of Defense, as a key player in the interagency effort, must rapidly respond to information attacks in coordination with a host of government departments and agencies, including the Departments of Commerce, Justice and State. It must be prepared to defend its own information and infrastructure; to support other government agencies in their defense, enforcement, and consequence management functions; and to counterattack with information operations weapons. This paper discusses the nature and level of the cyber threat and DoD's roles in countering it in an interagency environment. The paper also looks at the legal issues DoD must consider in planning and executing its information defense mission. It examines the current arrangement for protection of the nation's infrastructure and suggests there are organizational issues impeding the speed and effectiveness of the country's defense that must be addressed.

ACCESSION NUMBER: ADA390545

http://handle.dtic.mil/100.2/ADA390545

Seward, Andrew B. ***U.S. Strategic Information Operations: The Requirement for a Common Definition and Organizational Structure in Support of the Global War on Terrorism.*** Carlisle Barracks, PA: Army War College, 2004. 39p.

Abstract: Despite its lofty title as one of the national elements of power, the informational component is fundamentally misunderstood in concept, diffused in responsibility, and fragmented in application. In American society, the right to free speech has primacy and citizens have a healthy distrust of official government rhetoric. Thus, the second tier status of informational power is perhaps unsurprising. But in the war of ideas and ideals that is the current Global War on Terrorism (GWOT), strategic information

operations can be neither ignored nor allowed to languish. It is time to re-organize and focus information operations at a national strategic level and harness its potential. Kinetic military power, diplomacy, and America's economic might are critical to the GWOT, but similar success in strategic information operations is essential to creating lasting change. This paper reviews the current state of strategic information operations; discusses the lack of existing consensus regarding strategic information operations' definition, scope, and what it might accomplish; suggests a new model for strategic-level information operations; and compares and makes a recommendation from four options for better organizing information operations within the United States Government at the national strategic level in support of GWOT. These options are as follows: Create a New Department of Information within the Executive Branch, Assign Executive Agency Responsibility for Strategic Information to an Existing Department Secretary or Agency, Create a National Security Council Policy Coordination Committee for Information Operations, or leave the situation Status Quo.

ACCESSION NUMBER: ADA424404

http://handle.dtic.mil/100.2/ADA424404

Shaffer, Glen. ***Air Force Information Operations.*** Arlington, VA: Deputy Chief of Staff Air and Space Operations, 2002 18p.

Abstract: A briefing about information operations from the Phoenix Challenge 2002 Conference and Warfighter Day.

ACCESSION NUMBERS: ADA406441

http://handle.dtic.mil/100.2/ADA406441

Sherwin, Michael E. ***Naval Reserve Support to Information Operations Warfighting.*** Monterey, CA: Naval Postgraduate School, 2001. 60p.

Abstract: Since the mid-1990s, the Fleet Information Warfare Center (FIWC) has led the Navy's Information Operations (IO) support to the Fleet. Within the FIWC manning structure, there are in total 36 officer and 84 enlisted Naval Reserve billets that are manned to approximately 75 percent and located in Norfolk and San Diego Naval Reserve Centers. These Naval Reserve Force personnel could provide support to FIWC far and above what they are now contributing specifically in the areas of Computer Network Operations, Psychological Operations, Military Deception and Civil Affairs. Historically personnel conducting IO were primarily reservists and civilians in uniform with regular military officers being by far the minority. The Naval Reserve Force has the personnel to provide skilled IO operators but the lack of an effective manning document and training plans is hindering their opportunity to enhance FIWC's capabilities in lull spectrum IO. This research investigates the skill requirements of personnel in IO to verify that the Naval Reserve Force has the talent base for IO support and the feasibility of their expanded use in IO.

ACCESSION NUMBER: ADA396525

http://handle.dtic.mil/100.2/ADA396525

Sicoli, Peter A. ***Filling the Information Void: Adapting the Information Operation (IO) Message in Post-Hostility Iraq.*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2005. 73p.

Abstract: In meeting the challenges of post-hostility Iraq, the area of information operations (IO) has received a great deal of attention. Unlike combat operations, the center of gravity in post-conflict Iraq has been restoration of basic services and influencing public support and perception. Thus, in post-war conflict, IO, with the objective and means to promote legitimacy, reduce confusion, and influence a population, can reasonably be seen as the decisive operation. Unfortunately, there is substantial evidence that planners faced serious challenges during the transition to post-hostility operations in Iraq. This monograph seeks to add to the Army's understanding of IO by providing an in depth examination of five challenges faced by IO officers at the start of the post-hostility phase of operations in Iraq. This monograph will discuss the major principles contained in FM 3-13, Information Operations: Doctrine,

Tactics Techniques and Procedure, and examine whether doctrinal adjustments are needed to provide more effective guidance for IO officers facing the issues identified in the five problem areas.
ACCESSION NUMBER: ADA436260
http://handle.dtic.mil/100.2/ADA436260

Slavin, Jim. ***Close Access Information Operations.*** Carlisle Barracks, PA: Army War College, 2000. 23p.
Abstract: The information age comes with the challenge of implementing offensive information operations. As the United States executes the National Military Strategy, we must understand that our future threats may value information even more than we do. We have to further delineate responsibilities for conducting offensive information operations. With the technological security advances and reliance upon closed information systems, we must prepare an operational force that will be prepared to conduct close access offensive information operations. Finally, we must have the necessary intelligence collection for supporting such a force.
ACCESSION NUMBER: ADA378025
http://handle.dtic.mil/100.2/ADA378025

Smart, Antoinette G. ***Cyber Power Theory First, Then Information Operations.*** Washington, DC: National War College, 2001. 14p.
Abstract: The words we use to express ideas and concepts matter. To be present at the beginning of the twenty-first century, in the midst of an information age, with no theory of information operations (IO) seems disconcerting, at least on the surface. Think tanks, government research organizations, and learned individuals have all pointed to the need for a viable theory of IO, yet no such theory has emerged. Despite the lack of a theory or national strategy for IO, the U.S. military does have IO organizations, doctrine, and training. The Department of Defense has the Joint Information Operations Center (JIOC), which provides full-spectrum IO support to CINCs and CJTFs. Each military Department has its own Information Warfare Center (IWC), which provide IO support to their respective services AFIWC for the Air Force, Fleet IWC (FIWC) for the Navy, and Land Information Warfare Agency (LIWA) for the Army. The U.S. military now has IO units, with some services redesignating intelligence units as IO units. One example is the mass Air Force redesignation of its Intelligence Wing and subordinate squadrons. The U.S. military has both joint and service IO doctrine in some areas it is consistent, in other areas it is not. And there are many highly technological tools for IO, so of course there must be training. But there is no theory of IO from a national perspective. Carl von Clausewitz said that the primary purpose of theory is to clarify concepts and ideas that have become confused and entangled. A plethora of questions emerges from the apparent entropy surrounding the development of a theory of IO.
ACCESSION NUMBER: ADA 441637
http://handle.dtic.mil/100.2/ADA441637

Smith, David E. ***Bytes or Bullets: The Implications of Chaplaincy Involvement Within Information Operations.*** Carlisle Barracks, PA: Army War College, 2006. 21p.
Abstract: This paper will discuss the importance of information operations (IO) as an element of information policy within the context of military strategy. Recently the U.S. military has participated in numerous combat and peace-support operations. In the current fight the strategic/tactical main effort focuses on non-kinetic non-lethal means. In light of these operations the Army has changed the means by which it plans coordinates and executes information-operations (IO) and IO-effects. A recent change has been commanders requesting the Unit Ministry Team (UMT) to participate in IO. The UMT can provide a critical role in IO in the area of religion. In current operations religion may be a vulnerability or decision point in the fight. The UMT has involvement in humanitarian and civil military operations that has become a critical part in support of IO. The UMT does not have the doctrine or training to operate in the IO realm. Most UMTs do not have extensive comparative religion training. This paper will review the implications to the Army chaplaincy of the UMT participating in IO; understand the impact of UMT involvement in IO and

its affect on religious support and mission accomplishment. The paper will propose an expanded role for the UMT.
ACCESSION NUMBER: ADA448686
http://handle.dtic.mil/100.2/ADA448686

Staker, R. J. ***Achieving Systemic Information Operations for Australian Defence***. Salisbury, Australia: Electronics Research Laboratory, October 1999. 28p.
Abstract: This document describes a proposed program of research into theories, methodologies and techniques appropriate to achieving a systemic Military Information Operations capability for the Australian Defence Force. The major expected outcomes of this research are decision support aids relevant to Information Operations, contributions to the theory of Information Operations and contributions to IO Policy and Doctrine. The doctrine would include matters relating to the design of organisations that are capable of operating effectively in an Information Operations environment.
REPORT NUMBER: DSTO-TN-0235
ACCESSION NUMBER: ADA371754
http://handle.dtic.mil/100.2/ADA371754

_____. ***An Application of Checkland's Soft Systems Methodology to the Development of a Military Information Operations Capability for the Australian Defence Force.*** Canberra, Australia: Defence Science and Technology Organisation, March 1999. 30p.
Abstract: There is widespread concern throughout many advanced nations concerning the potential for Information Operations to influence the outcome of Military Operations. This concern is shared by elements of the Australian Defence Force and other Australian government agencies. In order to ensure that any such potential does not adversely affect Australian interests, there is a need to develop an Australian Military Information Operations capability. This document uses concepts from Checkland's Soft Systems Methodology to explore methods through which such a capability could be achieved.
REPORT NUMBER: DSTO-TN-0183
ACCESSION NUMBER: ADA362560
http://handle.dtic.mil/100.2/ADA362560

_____. ***Military Information Operations Analysis Using Influence Diagrams and Coloured Petri Nets.*** Salisbury, Australia: Electronics Research Laboratory, 1999. 78p.
Abstract: This report describes how Influence Diagrams, Coloured Petri Net models and related techniques may be used to analyse certain aspects of Military Information Operations. An example is employed to demonstrate these techniques. The example used is a very simplified representation of a Military Command Organisation dealing with a decision problem. The objective of the report is to provide theory, methods and techniques to support the assessment of the effect of Military Information Operations on such organisations. The simplicity of the example permits the basic concepts to be clearly conveyed. They may readily be extended to the analysis of more complex examples as required. The most fundamental and significant concept developed in this report is that of a common quantitative measure of effectiveness that encompasses all types of Information Operations relevant to Information Warfare. This permits the direct comparison of the effectiveness of alternative Information Operation options with one another and also with conventional operations options. This latter ability is essential if Information Operations are to be employed appropriately as part of a broader range of military options.
ACCESSION NUMBER: ADA373934
http://handle.dtic.mil/100.2/ADA373934

Steele, Robert D. ***Information Operations: Putting the 'I' Back Into Dime***. Carlisle Barracks, PA: Army War College, Strategic Studies Institute, 2006. 81p.

Abstract: The end of the Cold War and the emergence of terrorism; radicalized religion; the proliferation and commoditization of weapons of mass destruction (WMD); and the increased informational and economic power of Arabia, Brazil, China, India, Indonesia, Iran, Russia, and Venezuela, among others, have brought Information Operations (IO) to the forefront of the unified national security strategy. In the past year, IO has matured from an early emphasis on the protection of critical infrastructures and against electronic espionage, and is now more focused on content and on interagency information-sharing. The value of information all information, not only secret information and the value of global monitoring in all languages, 24/7, have been clearly established by the Undersecretary of Defense for Intelligence (USDI). This monograph defines and discusses three IO elements: " Strategic Communication (the message); " Open Source Intelligence (the reality); and, " Joint Information Operations Centers (the technology). These elements are further discussed in relation to six IO-heavy mission areas: " Information Operations generally; " Peacekeeping Intelligence (reactive); " Information Peacekeeping (proactive); " Early Warning (conflict deterrence, proactive counterterrorism); " Stabilization and Reconstruction Operations; and, " Homeland Defense and Civil Support.

ACCESSION NUMBER: ADA444640

http://handle.dtic.mil/100.2/ADA444640

Stewart, Michael J. ***Information Operations, Information Warfare: Policy Perspectives and Implications for the Force***. Carlisle Barracks, PA: Army War College, April 1997. 43p.

Abstract: Information Operations and Information Warfare are hot topics today and as a result, there is a tremendous amount of intellectual capital invested in the debate over what impact of new information technologies will have in two areas. These areas parallel two of our three components of the national security strategy; first is enhancing our security and the second is promoting prosperity. In many regards, the interests involved are somewhat mutually exclusive, which presents a challenging environment for issue identification and policy development. This paper identifies a few of the many scenarios in which information operations/warfare are a component; reviews some of the directions provided to the government as a whole and the military in particular; discusses why our nation is now more vulnerable to asymmetric attack; and then provides a few historical precedents. Finally, several of the many issue areas are analyzed, followed by the derivative implications for our military forces. The basic philosophical underpinning in this analysis is that solutions to these emerging issues must be consistent with our historical identity and values; failing this, we expose our long-term interests to unacceptable and probably fatal risk.

ACCESSION NUMBER: ADA326791

http://handle.dtic.mil/100.2/ADA326791

Straughan, Matt. ***Information Operations and Unity of Effort: The Case for a Joint Interagency Information Operations Task Force***. Newport, RI: Naval War College, Military Operations Department, June 1997. 26p.

Abstract: With the end of the Cold War and the resulting down-sizing of the military, unity of effort between all instruments of U.S. national power is more important than ever. Currently, the organizational structure does not exist to effectively and efficiently coordinate the instruments of power below the national-strategic or theater-strategic level of operations. By establishing a Joint Interagency Information Operations Task Force (JIIOTF) at the operational level, in support of military operations, including MOOTW, unity of effort and a coordinated application of the information instrument of power can be achieved. The result of coordinated InfoOps would be reduced combat casualties, faster establishment of legitimacy for humanitarian operations, increased host nation support for relief missions, and more effective application of the other instruments of power. ANNOTATION: Reprint: Information Operations and Unity of Effort: The Case for a Joint Interagency Information Operations Task Force.

ACCESSION NUMBER: ADA328145

http://handle.dtic.mil/100.2/ADA328145

Strawn, James C. ***Information Operations Challenges***. Carlisle Barracks, PA: Army War College, April 1998. 36p.

Abstract: This paper examines the need for a coherent and well-defined national strategy for information operations. The impetus is today's environment and the realities of the environment we will face as we enter the next century. The paper begins by evaluating the present environment and highlighting key factors that contribute to the imperative nature of this challenge followed by a review of the current status of national initiatives. Finally, the paper discusses key steps to be taken in this arena. The review of the present environment includes a macro-level look at the United States and its information needs. This look contrasts and compares the United States with its allies and its potential adversaries. With the review of the environment providing a foundation, a candid discussion of our nation's information operations initiatives helps to bring the issues into focus. The initiatives cannot be viewed solely from a Department of Defense perspective as they are addressing national challenges. These challenges share similarities with those in the arena of the asymmetric Weapons of Mass Destruction (WMD) threat. The solutions to those WMD threats demanded interagency and multi-national cooperation, the sarne is true for threats in cyber space.

ACCESSION NUMBER: ADA344942

http://handle.dtic.mil/100.2/ADA344942

Tatge, Aletha S. ***Perception Management and Coalition Information Operations*.** Monterey, CA: Naval Postgraduate School, 2001. 101p.

Abstract: This thesis focuses on the conduct of perception management (PM) within coalitions. Research has alluded to the possibility of predicting human behavior by creating stories that convey a believable reality. Further, does PM have any organizational process relationship with engagement planning? Target selection? Press statement coordination? The thesis focuses on how well coalitions are poised to conduct integrated PM operations. It identifies current PM capabilities by studying two recent coalition operations and determines how to best coordinate integration efforts. The purpose of this study is to analyze various methods of perception management and determine how they can be incorporated into current US Information Operations. One area of study will be the importance of credibility of our leaders when placed in a position of authority. This study will show that credibility is one of the toughest factors to achieve. A second area of study will be the value of story telling in gaining populace support and validation for intervening in conflicts that require the use of force and soldiers. As Stephen Pease said, "the message must be believable, though not necessarily true." (Stephen Pease 1950)

ACCESSION NUMBER: ADA396269

http://handle.dtic.mil/100.2/ADA396269

Thomas, Timothy L. ***Cyber Mobilization: The Neglected Aspect of Information Operations and Counterinsurgency Doctrine.*** Fort Leavenworth, KS: Foreign Military Studies Office, 2007. 23p.

Abstract: For over two years, the U.S. armed forces have focused on seeking ways to counter insurgent use of improvised explosive devices (IEDs) in both Afghanistan and Iraq. Less attention has been paid to countering the mobilization process that produces the seemingly unending line of insurgents willing to (1) become suicide bomber (walking IEDs or WIEDs), (2) prepare the IEDs, and (3) fight street battles. The insurgents use the Internet's "cyber mobilization" potential to fuel and supply this line of volunteers. They have been particularly successful in recruiting volunteers from other countries such as Saudi Arabia and Egypt. This success has forced coalition forces to continually react to the environment instead of controlling it.

ACCESSION NUMBER: ADA471028

http://handle.dtic.mil/100.2/ADA471028

Tulak, Arthur N. ***The Application of Information Operations Doctrine in Support of Peace Operations***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advances Military Studies, June 1999. 231p.

Abstract: This study investigates the application of Army Information Operations (IO) doctrine in a peace operations environment. Doctrinal concepts are applied to the category of military operations other than war (MOOTW) in general, and peace operations in specific. where possible, examples of doctrine in application in contingency operations are provided to amplify the doctrinal discussions. The study is built upon current doctrinal sources for joint and Army IO and its component disciplines, as well as active collection of observations and primary research on Task Force Eagle in Operations Joint Endeavor, Joint Guard, and Joint Forge in Bosnia-Herzegovina. The most frequent noncombat mission requiring IO has been peacekeeping and peace enforcement. Presently, there is no doctrinal source focused on implementing IO in peace operations. The study provides a starting point for a MOOTW-specific IO doctrine, identifying how the components of 10 are adapted to the special purpose of peace operations. Specific recommendations are provided for Army 10 doctrine and for the doctrines of the information-based disciplines supporting IO.

Tuner, Bunyamin. ***Information Operations in Strategic, Operational, and Tactical Levels of War: A Balanced Systematic Approach.*** Monterey, CA: Naval Postgraduate School, 2003. 75p.

Abstract: This thesis explores the idea whether a balanced systematic approach is a better way to integrate Information Operations (IO) at different levels of war compared to uncoordinated efforts at each level. Analysis of the role of information in a conflict in the context of information superiority provides the foundation of the thesis. DOD's IO core, supporting, and related capability based approach was used in the analysis of each level of warfare. Strategic, operational, and tactical level IO were analyzed by matching relevant IO capabilities with the IO effects desired at the respective levels. Sample systems were provided for each capability when appropriate. IO efforts in Operation Desert Storm and Operation Allied Force were analyzed. This thesis concluded that a balanced systematic approach to IO through its integration at all three levels of warfare will produce much better results than the uncoordinated cases in order to exploit the integrative effect of IO on the instruments of national power and the military capabilities at different levels of warfare.

ACCESSION NUMBER: ADA418305

http://handle.dtic.mil/100.2/ADA418305

http://bosun.nps.edu/uhtbin/hyperion-image.exe/03sep%5FTuner.pdf

Velasco, Diego. ***Full Spectrum Information Operations and the Information Professional Officer Intermediate Qualification Process: Filling the Gap to Ensure the Continued Leadership of the Information Professional Community in the Area of Information Dominance.*** Monterey, CA: Naval Postgraduate School, 2005. 59p.

Abstract: There currently exists a major effort within the United States Navy's Information Professional (IP) Community to overhaul and improve the qualification process for its officers. The overall effort has included the addition of technical refresher courses, re-examination of the Continuing Education Units (CEU) system, and the improvement of the Basic, Intermediate, and Advanced Qualification programs. This thesis specifically addresses the Intermediate Qualification (IQ) and the lack of Information Operations (IO) concepts therein. While some portions of the IQ that address highly technical areas exist, there is little to no mention of the importance of and concepts contained within IO, as defined by Joint Doctrine. The IP Community has a unique opportunity to train its officers in the concepts, competencies, and supporting activities of IO. This will ensure that the IP Community continues to be the Navy's leaders in the area of information dominance. This thesis provides recommended line items for injection into the IP IQ in the appropriate format with discussions and definitions that address the specific line items. The thesis also provides further recommendations for the continuing improvement and refinement of the IP qualification process, especially in the area of IO.

ACCESSION NUMBER: ADA439831

http://handle.dtic.mil/100.2/ADA439831
http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Sep%5FVelasco.pdf

Walker, Allisa M. ***Knowledge Portal Support to the Naval Postgraduate School's Advanced Distributed Learning Program for the Information Systems and Operations Curriculum.*** Monterey, CA: Naval Postgraduate School, 2000. 55p.

Abstract: The Naval Postgraduate School is in the process of migrating the Information Systems and Operations curriculum to a nonresident mode of delivery. Once the migration is complete, there will be a knowledge base available for use by battle staffs as well as policy and acquisition leaders. A knowledge portal may be the solution to facilitating the use of the knowledge base by both learners and operators. The goal of this research is to show how developing a knowledge portal for use with the Information Systems and Operations curriculum knowledge base could expand the use of tacit and explicit knowledge by the operators. By providing access to this repository of information and knowledge, users can capture the most up-to-date knowledge on issues in the world's political and military environment, have the ability to collaborate with experts in the field, and receive answers to questions that will aid in resolving complex issues.

ACCESSION NUMBER: ADA386259
http://handle.dtic.mil/100.2/ADA386259
http://bosun.nps.edu/uhtbin/hyperion-image.exe/00Dec_Walker.pdf

Waltz, Ed. ***Data Fusion in Offensive and Defensive Information Operations.*** Ann Arbor, MI: Veridian Systems Division, Inc., 2001. 15p.

Abstract: The conduct of offensive and defensive Information Operations (IO) require coordinated targeting and protection, respectively, across physical, information and even cognitive domains. Even the specific IO activities of Computer Network Defense (CND) and Computer Network Attack (CNA) require the close coordination of activities across all three domains to encompass physical processing assets, information creation, flows and stores, and the cognitive behaviors of human network administrators and operators. This paper describes the role of data fusion to provide intelligence for IO and to conduct both offensive operations (OIO) and defensive operations (DIO). We build on prior papers that have introduced the concept of a three-domain model of IO targets, and the general application of data fusion to the more abstract functions of IO. These functions require the fusion of both quantitative and qualitative data (e.g. numerical and text data, respectively) to develop models of physical, symbolic and cognitive IO targets and situations. This paper describes conceptual implementations of data fusion structures to model and understand OIO and DIO targets within the domains of reality.

ACCESSION NUMBER: ADA400192
http://handle.dtic.mil/100.2/ADA400192

Warren, Paul S. ***A New Kind of War: Adaptive Threat Doctrine and Information Operations.*** Fort Leavenworth, KS: Army Command and Staff College, 2001. 49p.

Abstract: The United States military remains the dominant post-modern state combatant. Military actions in Kosovo, Bosnia, and the Desert Storm victory validated the theory that information-based technologies are decisive factors in modern military operations. Threats recognize that peer competitors of the U.S. do not exist and are several decades away from developing similar military technologies. Consequently, threat-based strategies seek alternative or asymmetrical methods of warfare designed to exploit U.S. weaknesses and disrupt or paralyze the decision-making apparatus. Information operations provide opportunities to avoid direct contact with superior conventional forces and threat capabilities enhanced where qualitative gaps with opposing forces exist. The theoretical framework for the study is a model of information warfare that draws a distinction between "cyberwar" and "netwar," two components of information warfare that are structurally different. Using a hybrid of this model, the effectiveness of threat strategy using "netwar" to disrupt the decision-making process and create paralysis at the strategic and operational level can be determined. Understanding how the threat is adapting to knowledge-based warfare and U.S. military information dominance is vital to U.S. national interests. What methods are state

and non-state actors using to counter U.S. technological superiority? Can adaptive threat applications be developed that cause strategic and operational paralysis? If so, then are they successful in achieving threat end-states and are they designed to use information operations to gain a relative advantage? Can it be shown that future threats to the security of the United States can develop new ways, specifically "netwar" strategies, to attack and exploit U.S. military weaknesses?

ACCESSION NUMBER: ADA394428

http://handle.dtic.mil/100.2/ADA394428

Washington, Ollie, Jr. ***The Legal and Ethical Implications of Information Operations.*** Carlisle Barracks, PA: Army War College, 2001. 29p.

Abstract: Information Operations (I0) is a family of programs and tools that are used to deprive or disrupt an adversary's information and information systems while assuring the continued availability of your own. The technological tools of IO have been developed and implemented so rapidly that the domestic and international laws that should govern their use have not kept pace. Hackers, cyber criminals, terrorist and foreign spies are using tools such as computer network attack while domestic and international laws are insufficient to adequately patrol them. Further, there are ethical issues involved in the use of these IO tools that may not have been adequately debated, at least from a societal standpoint, to mediate possible conflicts with our national values. IO tools will allow the U.S. to engage and disable enemy facilities previously engaged with kinetic weapons, without the physical collateral damage, but with possible significant impact on noncombatants. International agreements such as the Geneva Convention do not specifically address IO and even within the U.S. military the rules of engagement on IO are not clear. This paper will attempt to explore some of these incongruities and provide a perspective on where the U.S. stance could be on our use of IO.

ACCESSION NUMBER: ADA390619

http://handle.dtic.mil/100.2/ADA390619

White Papers - 2025. Volume 1. Awareness. Maxwell AFB: Air University, Center for Aerospace Doctrine Research and Education, 1996. 342p.

Abstract: A robust information operations architecture can provide leaders dominant battlespace knowledge and tools for improved decision making. US armed forces in 2025 need an information operations system that generates products and services that are timely, reliable, relevant, and tailored to each user's needs. The products must come from systems that are secure, redundant, survivable, transportable, adaptable, deception resistant, capable of fusing vast amount of data, and capable of forecasting. The information operations architecture of 2025 proposed in this paper consists of thousands of widely distributed nodes performing the full range of collection, data fusion, analysis, and command functions-all linked together through a robust networking system. Data will be collected, organized into usable information, analyzed and assimilated, and displayed in a form that enhances the military decision maker's understanding of the situation. The architecture will also apply modeling, simulation, and forecasting tools to help commanders make sound choices for employing military force. This architecture allows the United States (US) armed forces to conduct Wisdom Warfare. The system can be used by the commander in chief, unit commander, supervisor, or technician. Somewhere in the workplace, in a vehicle, or on the person there will be a link to the sensors, transmitters, receivers, storage devices, and transformation systems that will provide, in push or pull fashion, all the synthesized information needed to accomplish the mission or task. Information will be presented in a variety of forms selected by the user.

ACCESSION NUMBER: ADA319864

http://handle.dtic.mil/100.2/ADA319864

White, Randall L. ***Command & Control Structures for Space and Information Operations in a Joint Command.*** Maxwell AFB, AL: Air University, Air Command and Staff College, 2002. 43p.

Abstract: ***This research develops two products for aiding a Joint Force Commander (JFC) tasked with developing command and control (C2) structures for space and information operation (IO) capabilities within a joint force. The first product is a decision matrix based upon two ideas essential to command and control. The first idea is that knowing the level of desired effect, that is, a strategic, operational, or tactical effect produced by space or IO functions is critical to the C2 structure. The second idea is that the JFC must determine which is more important, the integration of functional capabilities into a single mission oriented team or the preservation of functional identities due to high demand/low density resources, the need to preserve critical functional expertise, or other related reasons which drive functional organizations. The second product of this research is a proposed core set of C2 structures across the three levels of command that can be adapted to the situation confronting a JFC. The core C2 structures lean toward the idea that space and IO be integrated with service capabilities in all Defense Departments rather than segregated into combatant commands or functional components independent from existing service organizations. The decision matrix and core C2 structures are based upon my analysis of service and joint doctrine and a case study I conducted on CENTCOMs employment of forces while conducting Operation Enduring Freedom in Afghanistan.***

ACCESSION NUMBER: ADA420647

http://handle.dtic.mil/100.2/ADA420647

Williamson, Jennie M. ***Information Operations: Computer Network Attack in the 21st Century.*** Carlisle Barracks, PA: Army War College, 2002. 29p.

Abstract: ***U.S. Information systems and critical infrastructures are vulnerable to attacks. The Department of Defense must establish directives to defend the U.S. information systems and critical infrastructures. The United States must devise measures to protect its citizens, critical infrastructures, and computer systems. The 21st century is more dynamic, with potential threats capable of launching cyber warfare via multiple means, targeting key United States' centers of gravity. Therefore, the United States must design a comprehensive computer network attack policy to deter potential adversaries. This study addresses current information operations policy, DoD roles and responsibilities, Computer Network Attack Concept and Strategy. Lastly, this report outlines the ends, ways and means of a computer network attack policy, designed to protect and sustain national security. The study highlights the current U.S. information operations policy as it relates to computer network attack. Further, the study describes why the U.S. must protect its information systems and critical infrastructures against potential attacks.***

ACCESSION NUMBER: ADA402018

http://handle.dtic.mil/100.2/ADA402018

Wingfield, Thomas C. ***Legal Aspects of Offensive Information Operations in Space***. Washington, DC: Department of Defense, 2005. 17p.

Abstract: What, then, are the specific steps to follow in performing a legal analysis of offensive information operations in space? First, correctly identify the type and subtype of operation contemplated. The three types are intelligence collection, offensive operations through satellites, and offensive operations against satellites. The subtypes for each are listed in the second section of this paper. Second, determine if this type of operation, in the light of all relevant circumstances, rises to the level of a use of force. Although international legal academics are only now turning to this question, the one settled concept in this area is that an information operation crosses the Article 2(4) threshold when it produces effects comparable to those of a kinetic attack which would be thought of as having crossed the threshold. What more than that would constitute a use of force is still an open question. If the action is the

equivalent of a use of force, it may only be undertaken pursuant to Chapter VII authorization, or as a lawful exercise of self-defense. Assuming the legality of acting at all, the operation must be conducted in accordance with the customary international legal standards of proportionality, discrimination, and chivalry. Offensive information operations in space will drive a revolution in technical, tactical, and legal thought. It is for the attorney adviser to the warfighter to present honest, closely reasoned legal advice to his client so that he may fight honorably and effectively.

ACCESSION NUMBER: ADA435835

http://handle.dtic.mil/100.2/ADA435835

Yingling, Paul L. ***Using the Targeting Process to Synchronize Information Operations at the Tactical Level.*** Fort Leavenworth, KS: Army Command and Staff College, 2002 67p.

Abstract: *The U.S. Army's new capstone doctrine, Field Manual (FM) 3-0, Operations, recognizes that information is a powerful weapon in the conduct of full-spectrum operations. Like other weapons, the effects of information must be synchronized with the effects of other systems to produce optimal results. Unfortunately, current U.S. Army doctrine does not provide a single coherent method for integrating the effects of maneuver, fires and information. This monograph seeks to remedy that flaw by analyzing the utility of the targeting process as a means of synchronizing information with the other elements of combat power at the tactical level. The decide-detect-deliver-assess (D3A) methodology of the targeting process is a useful conceptual tool for synchronizing effects on hostile forces. However, in practice the targeting process contains a bias towards lethal effects. With minor modifications, the targeting process could become a far more effective synchronization tool.*

ACCESSION NUMBER: ADA403848

http://handle.dtic.mil/100.2/ADA403848

Information Assurance

Books

Burrows, Robert, et al. “Issues in Operational Test and Evaluation of Information Assurance Vulnerabilities.” p. 251-253, IN: **Proceedings of the 1998 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 29 June - 1 July 1998. Washington, DC: National Defense University, 1998. 943p.
DKL UB212 .C68 1998 GENERAL

Gansler, Jacques S. and Hans Binnendijk. **Information Assurance: Trends in Vulnerabilities, Threats, and Technology.** Washington, DC: National Defense University, Center for Technology and National Security Policy, 2004. 146p.
http://www.ndu.edu/ctnsp/IA_final.pdf
DKL QA76.9 .A25 I74 2004 GENERAL

Kennedy, Kevin J. **Grand Strategy for Information Age National Security: Information Assurance for the Twenty-First century**. Maxwell Air Force Base, AL: Air University Press, [1997]. 86p.
http://handle.dtic.mil/100.2/ADA329104
DKL U163 .K46 1997 GENERAL

Proceedings of the 10th International Command and Control Research and Technology Symposium. “Track 7 Information Operations/Assurance.” Vienna, VA, 13-16 June 2005. Washington, DC: National Defense University, 2005.
http://www.dodccrp.org/events/10th_ICCRTS/CD/foreword.htm

United States. Dept. of Defense. Office of the Inspector General. **Information Assurance of the Defense Civilian Personnel Data System - Navy.** Audit Report No. 98-127. Arlington, VA: Inspector General, Dept. of Defense, 1998. 31p.
http://www.dodig.osd.mil/audit/reports/fy98/98-127.pdf

United States. General Accounting Office. National Security and International Affairs Division. **DOD's Information Assurance Efforts**. GAO/NSIAD-98-132R. Washington, DC: The Office, [1998]. 7p.
http://archive.gao.gov/paprpdf2/160631.pdf

United States. Joint Chiefs of Staff. **Information Assurance: Legal, Regulatory, Policy and Organizational Considerations**. Eds. 1-4. Washington, DC: Joint Chiefs of Staff, 1997-1999.
DKL D 5.2: IN 4/2 FEDDOCS [4th ed]
DKL D 5.2: IN 3/2 FEDDOCS [3rd ed]
DKL U260 .I53 1996 GENERAL [2nd ed]
DKL U260 .I53 1995 GENERAL [1st ed]
http://handle.dtic.mil/100.2/ADA316285

Periodicals

Barker, Larry. “Information Assurance: Protecting the Army’s Domain-Name System.” **Army Communicator**, Summer 2001, v. 26, no. 2, p. 39-41.

Campen, Alan D. “Low-Tech Humans Subvert High-Tech Information Assurance.” **Signal**, January 2002, v. 56, no. 5, p. 37-39.

Carter, Ashton, et al. “Catastrophic Terrorism.” **Foreign Affairs**, November/December 1998, v. 77, no. 6, p. 80-94.

Cothron, Robert. “Information Assurance & Military Treatment Facilities.” **TIG Brief - The Inspector General**, Summer 2006, v. 58, no. 3, p. 18-19.

Deal, John C., Michael F. Brown, and Phillip J. Loranger. “Information Assurance in the Information Age.” **Army AL&T**, September-October 1999, v. 99, no. 5, p. 9-10.

Duerr, Thomas, Nicholas D. Beser and Gregory P. Staisiunas. “Information Assurance Applied to Authentication of Digital Evidence.” **Forensic Science Communications**, October 2004, v. 6, no. 4.
http://www.fbi.gov/hq/lab/fsc/backissu/oct2004/research/2004_10_research01.htm

Good, Travis. “Army Reserve Trains for Information Assurance.” **Signal**, January 2004, v. 58, no. 5, p. 53-56.

Hancock, Bill. “NSA Goes Commercial – Eval Services Part of the Offering.” **Computers & Security**, 1999, v. 18, no. 8, p. 651-652.

Jones, Harry E., II. “Information Dominance for Army XXI: Battlefield Visualization.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no, 1, p. 8-10.

Jones, Michael D. “CCIR: A Tool for Information Dominance [Commander’s Critical Information Requirements].” **Military Review**, March-April 2001, v. 81, no. 2, p. 25-29.

Kenyon, Henry S. “Keeping Malicious Code at Bay.” **Signal**, August 2002, v. 56, no. 12, p. 29-32.

Lawlor, Maryann. “Intelligence Agency Boosts Information Security IQ.” **Signal**, August 2005, v. 59, no. 12, p. 17+

McKendrick, Joseph. “Diverse Groups Share Information Assurance Quandaries.” **Signa**l, August 2002, v. 56, no. 12, p. 41-44.

Nifong, Michael R. “Key to Information Dominance.” **Military Review**, May-June 1996, v. 76, no. 3, p. 62-67.

Seffers, George I. “Civilian Agencies May Adopt DoD Security System.” **Federal Times**, November 15, 1999, v. 35, no. 41, p. 4.

Turk, Robert and Shawn Hollingsworth. “Information Assurance: Army Prepares for Next Generation of Warfare.” **Army Communicator**, Spring 2000, v. 25, no. 1, p. 34-35.

Voas, J. “Protecting Against What? The Achilles Heel of Information Assurance.” **IEEE Spectrum**, January-February 1999, v. 16, no. 1, p. 28-29.

Watt, Glenn D. “Self-Inflicted System Malfunctions Threaten Information Assurance.” **Signal**, July 1999, v. 53, no. 11, p. 61-63.

Welch, Donald, Daniel Ragsdale and Wayne Schepens. “Training for Information Assurance.” **Computer**, April 2002, v. 35, no. 4, p. 30-37.

Winter, Steven and David E. Sterling. “GuardRail Pilot Program--A Legacy of Teaming: Rapid Response Information Dominance [airborne signal intelligence collection and location system].” **Program Manager**, September-October 2000, v. 29. no. 5, p. 80-82. *http://www.dau.mil/pubs/pm/pmpdf00/Wins-o.pdf*

Documents, Theses & Technical Reports

Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography.

Beauregard, Joseph E. ***Modeling Information Assurance***. Wright Patterson AFB, OH: Air Force Institute of Technology, School of Engineering and Management, 2001. 223p.
Abstract: The ever-increasing speed of information systems allows decision-makers around the world to gather, process, and disseminate information almost instantaneously. However, with this benefit there comes a price. Information is valuable and therefore a target to those who do not have it or wish to destroy it. The Internet has allowed information to flow freely, but it has also made information vulnerable to many forms of corruption. The U. S. military controls much of the world's most sensitive information, and since it cannot sacrifice losing the speed at which this information is currently processed and disseminated, it must find a way to assure its protection. There has been some effort to model information assurance in recent years, however the no accepted quantifiable model currently exists. This study presents a strategy to aid organizations, specifically organizations within the Department of Defense (DoD), in their efforts to protect valuable information and information systems. The model is reviewed and results from an actual analysis are presented.
ACCESSION NUMBER: ADA390985
http://handle.dtic.mil/100.2/ADA390985

Brodhun, III, Carl P. ***Prioritization of Information Assurance (IA) Technology in a Resource Constrained Environment.*** Monterey, CA: Naval Postgraduate School, 2001. 120p.
Abstract: Classical risk analysis is a static process that does not account for rapid evolutionary or generational changes in technology and technological solutions. This thesis defines a process that expands classical risk analysis to increase visualization of the security environment of an information system. It provides a comparative analysis of system attributes and encourages focused communications between decision-makers and information systems technicians. Personal interviews with domain experts from four organizations were used to construct a baseline model. Face validity of the model was determined during sessions with the domain experts. The model was calibrated to two specific scenarios using a pair of surveys to set link values and establish data for the initial nodes. A verification phase compared rough results from the model with expert opinion. The model evaluated, prioritized and graphically illustrated shortfalls within two information systems based on the relative importance of specific criteria established by the domain experts. It facilitated the extraction of implicit or tacit knowledge from the domain experts that would not emerge during a classical risk analysis.
ACCESSION NUMBER: ADA457789
http://handle.dtic.mil/100.2/ADA457789
http://bosun.nps.edu/uhtbin/hyperion-image.exe/01Dec%5FBrodhun.pdf

Cone, Benjamin D. ***A CYBERCIEGE Campaign Fulfilling Navy Information Assurance Training and Awareness Requirements.*** Monterey, CA: Naval Postgraduate School, 2006. 279p.
Abstract: The broad use of information systems within organizations has led to an increased appreciation of the need to ensure that all users be aware of basic concepts in Information Assurance (IA). The Department of Defense (DOD) addressed the idea of user awareness in DOD Directive 8750.1. This directive requires that all users of DOD information systems undergo an initial IA awareness orientation followed by annual refresher instruction. This thesis created a CyberCIEGE campaign for the

Naval Postgraduate School's CyberCIEGE project that will fulfill Navy requirements to meet DOD Directive 8750.1. The first portion of this thesis is an analysis of four IA programs and products. Requirements for Navy IA awareness and training products were developed from this analysis. The second part of this thesis is a description of two CyberCIEGE scenarios that were created to fulfill these requirements. The first scenario focuses on basic IA awareness and emphasizes information that the Navy should reinforce. The scenario is intended for all users of Navy information systems. The second scenario is intended for technical users and addresses more advanced concepts and technical considerations. The technical user scenario emphasizes skill application and problem solving.

ACCESSION NUMBER: ADA445392

http://handle.dtic.mil/100.2/ADA445392

http://bosun.nps.edu/uhtbin/hyperion-image.exe/06Mar%5FCone.pdf

Deschaine, Darren A. ***An Analysis of Biometric Technology as an Enabler to Information Assurance.*** Wright Patterson AFB, OH: Air Force Institute of Technology, School of Engineering and Management, 2005. 75p.

Abstract: The use of and dependence on, Information technology (IT) has grown tremendously in the last two decades. Still, some believe the United States is only in the infancy of this growth. This explosive growth has opened the door to capabilities that were only dreamed of in the past. As easy as it is to see how advantageous this technology is, it also is clear that with its advantages come distinct responsibilities and new problems that must be addressed. For instance, the minute one begins using information processing systems, the world of information assurance (IA) becomes far more complex. As a result, the push for better IA is necessary. To reach this increased level of IA, a further dependence on technology has developed. As an example, the field of biometrics has matured and has become an enabler to the U.S. Department of Defense IA model.

ACCESSION NUMBER: ADA434466

http://handle.dtic.mil/100.2/ADA434466

Fox, Jonathan M. ***Information Assurance and the Defense in Depth: A Study of Infosec Warriors and Infosec Cowboys.*** Fort Leavenworth, KS: Army Command and General Staff College, 2003. 161p.

Abstract: This study investigates the Army's ability to provide information assurance for the NIPRNET. Information assurance includes those actions that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. The study examines how the military's defense in depth policy provides information assurance with a system of layered network defenses. The study also examines current practices used in the corporate world to provide information assurance. With the cooperation of the Human Firewall Council, the study compared the performance of four organizations according to standards developed for the Council Council's Security Management Index. The four participants in the study included: an Army Directorate of Information Management, a government agency, a university, and a web development company. The study also compared the performance of the four participants with the aggregate results obtained by the Human Firewall Council. The study concluded the defense in depth policy does grant the Army an advantage over other organizations for providing information assurance. However, the Army would benefit from incorporating some of the common practices of private corporations in their overall information assurance plans.

ACCESSION NUMBER: ADA416561

http://handle.dtic.mil/100.2/ADA416561

Friedman, Arthur R. ***A Way to Operationalize the DOD's Critical Infrastructure Protection Program Using Information Assurance Policies and Technologies.*** Carlisle Barracks, PA: Army War College, 2005. 35p.

Abstract: The Department of Defense (DoD) Defense Critical Infrastructure Protection Program has recently reorganized under the Office of the Assistant Secretary of Defense for Homeland Defense under

the Under Secretary of Defense for Policy. Requirements have been set forth in DoDD 3020.ff Defense Critical Infrastructure which is in final coordination and is anticipated to be published later this fiscal year. This policy states that Defense Critical Infrastructure and non-DoD infrastructures are essential to planning mobilizing deploying and sustaining military operations within the U.S. as well as globally shall be available when required. Today's Combatant Commanders do not have the ability to quickly and efficiently share information that identifies critical infrastructure assets and single points of failure to prevent physical or cyber attacks from impairing the Global Information Grid. The intent of this paper is to provide a construct to Operationalize the DoD's Critical Infrastructure Protection Program through the use of Information Assurance policies methodologies and technologies and to identify strategic implications of vulnerabilities to the Combatant Commander and supporting agencies.

ACCESSION NUMBER: ADA431755

http://handle.dtic.mil/100.2/ADA431755

Garvin, John R. and Peter H. Christensen. ***USMC Information Assurance Operational Testing and Training Strategy.*** Quantico, VA: Marine Corps Operational Test and Evaluation Activity, 2001. 27p.

Abstract: This briefing discusses MCOTEA's mission and scope, the USMC's high interest programs, cyber threat and network centric warfare, information assurance and joint interoperability.

ACCESSION NUMBER: ADA399993

http://handle.dtic.mil/100.2/ADA399993

Giovannetti, Robert G. ***An Analysis of Information Assurance Relating to the Department of Defense Radio Frequency Identification (RFID) Passive Network.*** Wright-Patterson AFB, OH: Air Force Institute of Technology, 2005. 66p.

Abstract: The mandates for suppliers to commence Radio Frequency Identification tagging set by Wal-Mart and the Department of Defense is changing this long-time rumored technology into reality. Despite the many conveniences to automate and improve asset tracking this technology offers, consumer groups have obstinately opposed this adoption due to the perceived weaknesses in security and privacy of the network. While the heated debate between consumers and retailers continues, little to no research has addressed the implications of security on the Department of Defense Radio Frequency Identification network. This thesis utilized a historical analysis of Radio Frequency Identification literature to determine whether the current network design causes any serious security concerns adversaries could exploit. The research concluded that at the present level of implementation, there is little cause for concern over the security of the network, but as the network grows to its full deployment, more evaluation and monitoring of security issues will require further consideration.

ACCESSION NUMBER: ADA434410

http://handle.dtic.mil/100.2/ADA434410

Gorodetski, Vladimir I., Victor A. Skormin, and Leonard J. Popyack***. Information Assurance in Computer Networks: Methods, Models and Architectures for Network Security.*** St. Petersburg, Russia: Russian Academy of Sciences, 2001.

Abstract: This volume contains the papers selected for presentation at the International Workshop on Mathematical Methods, Models and Architectures for Network Security Systems (MMM-ACNS 2001) held in St. Petersburg, Russia on May 21-23, 2001. The workshop was organized by the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in cooperation with the Russian Foundation for Basic Research (RFBR), the U.S. Air Force Research Laboratory and the U.S. Air Force Office of Scientific Research. The workshop focus was on mathematical aspects of information and computer network security and the role of mathematical issues in contemporary and future development of models of secure computing. Topics included: mathematical models for computer networks and applied system security; methods and models for intrusion detection; mathematical basis and applied techniques of cryptography and steganography; applied techniques of cryptography and models for access control, authentication and authorization.

ACCESSION NUMBER: ADA396962
http://handle.dtic.mil/100.2/ADA396962

Guild, R. James. ***Design and Analysis of a Model Reconfigurable Cyber-Exercise Laboratory (RCEL) for Information Assurance Education.*** Monterey, CA: Naval Postgraduate School, 2004. 109p.

Abstract: This thesis addresses the need to create a flexible laboratory environment for teaching network security. For educators to fully realize the benefit of such a facility, prototype exercise scenarios are also needed. The paper is based on a model laboratory created at the Naval Postgraduate School. The initial configuration of the NPS lab is described. The work then develops a list of learning objectives achievable in the kCEL. Six prototype cyber-exercise scenarios are presented to supplement the kCEL description. The activities within each potential scenario are described. The learning objectives met during each scenario are shown. This work demonstrates how a variety of potential kCEL exercises can supplement traditional information assurance education delivery techniques.

ACCESSION NUMBER: ADA422241
http://handle.dtic.mil/100.2/ADA422241
http://bosun.nps.edu/uhtbin/hyperion-image.exe/04Mar%5FGuild.pdf

Gumke, Randall. ***Navy/Marine Corps Intranet Information Assurance Operational Services Performance Measures.*** Monterey, CA: Naval Postgraduate School, 2001. 130p.

Abstract: Communicating in the Department of the Navy (DON) over the Internet is an everyday event. The DON is developing the Navy Marine Corps Intranet (N/MCI) to enhance this communication capability. The security of communicating over the N/MCI has become a concern to the DON. The DON is relying on the N/MCI contractor to provide security for their communications. Key aspects of this secure communication will be provided through the use of a DON Public Key Infrastructure (PKI), which the N/MCI contractor is managing. To ensure the security of the PKI based communications the contract requires the monitoring of four PKI performance measures. This thesis analyzes performance measures, criterion, and standards then uses this analysis to review the contractual PKI performance measures and data collected from commercial PKI vendors. It recommends changes to these performance measures and provides additional performance criteria that should be included in the N/MCI contract. Finally, this thesis analyses how the N/MCI contract, specifically the PKI, impact DON members.

ACCESSION NUMBER: ADA396135
http://handle.dtic.mil/100.2/ADA396135
http://bosun.nps.edu/uhtbin/hyperion-image.exe/01Jun_Gumke.pdf

Hart, James L. M. ***An Historical Analysis of Factors Contributing to the Emergence of the Intrusion Detection Discipline and its Role in Information Assurance.*** Wright Patterson AFB, OH: Air Force Institute of Technology, School of Engineering and Management, 2005. 81p.

Abstract: In 2003, Gartner, Inc., predicted the inevitable demise of the intrusion detection (ID) market, a major player in the computer security technology industry. In light of this prediction, IT executives need to know if intrusion detection technologies serve a strategic purpose within the framework of information assurance (IA). This research investigated the historical background and circumstances that led to the birth of the intrusion detection field and explored the evolution of the discipline through current research in order to identify appropriate roles for IDS technology within an information assurance framework. The research identified factors contributing to the birth of ID including increased procurement and employment of resource-sharing computer systems in the DoD, a growing need to operate in an open computing environment while maintaining security and the unmanageable volume of audit data produced as a result of security requirements. The research also uncovered six trends that could be used to describe the evolution of the ID discipline encompassing passive to active response mechanisms, centralized to

distributed management platforms, centralized to distributed/agent-based detection, single to multiple detection approaches within a system, host-based to network to hybrid analysis and software-based to hardware-based/in-line devices. Finally, the research outlined three roles suitable for IDS to fulfill within the IA framework including employing IDS as a stimulus to incident response mechanisms, as a forensic tool for gathering evidence of computer misuse and as a vulnerability assessment or policy enforcement facility.

ACCESSION NUMBER: ADA434323

http://handle.dtic.mil/100.2/ADA434323

Jorgensen, Jane and Philippe Rossignol. ***Information Assurance Cyber Ecology***. Arlington, VA: IET Corporation, 2003. 211p.

Abstract: Cyber Ecology is a systems-level discipline addressing the emergent properties of computer networks and their responses to perturbations, such as attacks. It is a cross-disciplinary synthesis incorporating elements of biology, epidemiology, ecology, computer science, and system engineering. In this work, methodologies from epidemiology and ecology were applied to information assurance. The goals of the Cyber Ecology project were to: (1) enable and demonstrate the discovery of noel IA technologies for the detection and mitigation of damage due to cyber attack through the application of ecological models, (2) design, develop, document, evaluate and deliver methodologies to assess the behavior of computer networks from attacks by infectious agents and direct attacks, and (3) develop and demonstrate methods to make system-level assessments about network health. The work in this report spans four major areas: (1) definition and scope of Cyber Ecology, (2) application of ecological concepts to the classification of malicious code, in which insider threat is briefly discussed, (3) epidemiological applications of Cyber Ecology, and 94) system health expressed as emergent properties that can be assessed through evaluation of network (community) structure.

ACCESSION NUMBER: ADA411943

http://handle.dtic.mil/100.2/ADA411943

Kaczor, William, Craig Thornley and Buddy Guynn. ***Taking the Mystery out of Information Assurance for the 21st Century Training Community.*** Orlando, FL: MTS Technologies, 2006. 10p.

Abstract: Information Assurance "IA" is one of the most overlooked yet critical aspects of any Information Technology "IT" system. Although IA applies to every IT system, we will focus on its application to simulators and any IT powered training device connecting to a DoD network. IA is the overarching process consisting of Computer/Network/Data/Information Security. If IA is built into every training and education system, and maintained throughout its life cycle, it is guaranteed to lower compromising threats to DoD assets. This paper will take the mystery out of IA, system security engineering, and the security Certification and Accreditation "C&A" process from both government and industry perspectives. It will provide proven solutions to achieve C&A on any system under differing conditions and time frames, and document the process of IA using proven systems security engineering processes, the DoD Information Technology Security Certification and Accreditation Process "DITSCAP", and the documentation strategy of using the System Security Authorization Agreement "SSAA" and the System Security Plan "SSP". This paper will also provide examples of Information Assurance Vulnerability Alerts "IAVAs", including how they work and greatly reduce the risk to all IT systems. It will present the best practices for new systems, blended certification approaches, how to certify legacy systems, and the proper end of life disposal. The 21st century force is moving more toward a net-centric, real time, and IT-based integrated operational and training environment. To achieve war-fighting excellence, IA of computer systems and networks should be a major focus of all new system designs for protection of national defense information and assets.

ACCESSION NUMBER: ADA474222

http://handle.dtic.mil/100.2/ADA474222

Kang, George S. and Yvette Lee. ***Voice Biometrics for Information Assurance Applications.*** Washington, DC: Naval Research Laboratory, 2002. 43p.

Abstract: In 2002, the President of the United States established an organization within the DOD to develop and promulgate biometrics technologies to achieve security in information, information systems, weapons, and facilities. NRL has been tasked to study voice biometrics for applications in which other biometrics techniques are difficult to apply. The ultimate goal of voice biometrics is to enable the use of voice as a password. Voice biometrics are "man-in-the-loop" systems in which system performance is significantly dependent on human performance. This aspect has not been properly emphasized by previous researchers in this field. Accordingly, we let each speaker choose his (or her) own test phrase that can be uttered consistently. The speech waveform is then pre-processed (i.e, equalized and normalized) to reduce the effect of inconsistent speaking. Subsequently, we extract five different voice features from the speech waveform. Some of them have never been used for voice biometrics. Finally, individual feature errors are combined to indicate a confidence level of speaker verification. Initial laboratory testing under various conditions shows encouraging results. We will be prepared to fleet-test our voice biometrics system in FY03.

ACCESSION NUMBER: ADA408449

http://handle.dtic.mil/100.2/ADA408449

Labert, Matthew J. ***Implementation of Information Assurance Risk Management Training into Existing Department of the Navy Training Pipelines.*** Monterey, CA: Naval Postgraduate School, 2002. 140p.

Abstract: With the implementation and continuing research on information systems such as Information Technology for the 21st Century (IT-21) Navy-Marine Corps Intranet (NMCI), and "Network-Centric warfare" there is little doubt that the Navy is becoming heavily dependent on information and information systems. Though much has been accomplished technically to protect and defend these systems an important security issue has thus far been overlooked the human factor. Information Assurance Risk Management (IARM) was a proposal to standardize the way DON personnel discuss, treat, and implement information assurance. IARM addresses the human security aspect of information and information systems in a regimented way to be understandable through all levels of the DON. To standardize the way DON personnel perceive information assurance, they must be taught what IARM is and how to use it. Can an IARM course be implemented in the DON, and if so, at what level and to who m should it be taught?

ACCESSION NUMBER: ADA401711

http://handle.dtic.mil/100.2/ADA401711

http://bosun.nps.edu/uhtbin/hyperion-image.exe/02Mar_Labert.pdf

Lamm, George A. ***Assessing and Managing Risks to Information Assurance: A Methodological Approach.*** Charlottesville, VA: University of Virginia, 2001. 306p.

Abstract: Recent events such as the Yahoo! denial-of-service attack and the I Love you virus have sparked a dramatic interest in information assurance (IA) and the future security of information infrastructures. Information systems are facing an increase in interconnectedness, interdependency and complexity. Information assurance attempts to answer critical questions of trust and credibility associated with our digital environment and it represents a myriad of considerations and decisions that transcend technological advancement, legal, political, economic, social, cultural, institutional, organizational, and educational dimensions. Despite spending millions of dollars on firewalls, encryption technologies, and intrusion detection software, information infrastructure vulnerabilities and incidents continue to happen. These trends have a significant impact on military operations in the next decades.

ACCESSION NUMBER: ADA391850

http://handle.dtic.mil/100.2/ADA391850

Lentz, Robert. ***Information Assurance and DoD: A Partnership with Industry.*** Washington, DC: Assistance Secretary of Defense, (Command, Control, Communications and Intelligence), 2002. 22p.

Abstract: This briefing presents the information assurance environment, DoD's vision, the DoD IA community response and challenges, the DoD Industry Relationship, key influences on the DoD and a summary.

ACCESSION NUMBER: ADA406432

http://handle.dtic.mil/100.2/ADA406432

Li, Xiaohua. ***Wireless Information Assurance and Cooperative Communications***. Binghamton, NY: State University at Binghamton, 2006. 24p.

Abstract: This report consists of four parts. The first part develops physical-layer security techniques with both multi-input single- output (MISO) transmissions and multi-input multi-output (MIMO) transmissions. The second part addresses cooperative communications, whereas the third part involves the testbed development. The final part contains conclusions.

ACCESSION NUMBER: ADA449197

http://handle.dtic.mil/100.2/ADA449197

Liu, Peng. ***Measuring Quality of Information Assurance (QoIA).*** University Park, PA: Pennsylvania State University, 2003. 36p.

Abstract: Current information assurance techniques do not allow us to state quantitatively how assured our systems and networks are. As a result, (a) security and assurance measures can only be designed and built into information systems in an ad hoc fashion, (b) it is difficult to characterize the capabilities of security measures, and (c) information systems cannot deliver quality of information assurance (QoIA) guarantees. This seedling project had two objectives: (1) to explore an economics theoretic framework for measuring assurance and (2) to explore a theory of QoIA management. For each objective, the study defines the problem space, offers some potentially feasible solutions, and creates a technology development roadmap for a 5 to 7 year time horizon. The key idea is to use incentive-based, economic models of attacker intent, objectives and strategies (AIOS) to measure a system's overall assurance capacity. As a result, a preliminary framework for AIOS modeling and inference is developed along with an approach which uses AIOS inferences to measure a system's assurance capacity. Two real-world assurance measuring case studies were conducted. Finally, a preliminary framework for measuring QoIA and delivering QoIA services in mission critical database systems is proposed.

ACCESSION NUMBER: ADA419205

http://handle.dtic.mil/100.2/ADA419205

Luiijf, H. A. M. ***Survey of Information Warfare, Information Operations and Information Assurance.*** The Hague, Netherlands: Fysisch en Elektronisch Laboratory, 1999. 92p.

Abstract: Research survey on the phenomena Information Warfare, Information Operations (Info Ops) and Information Assurance. History, development, definitions and developments in various countries around the globe. Appendix with list of abbreviations of terms in these fields.

ACCESSION NUMBER: ADA367670

http://handle.dtic.mil/100.2/ADA367670

May, Chris, et al. ***Advanced Information Assurance Handbook.*** Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute, 2004. 282p.

Abstract: This handbook is for technical staff members charged with administering and securing information systems and networks. The first module briefly reviews some best practices for securing host systems and covers specific techniques for securing Windows 2000 and Red Hat Linux systems. It also

discusses the importance of monitoring networked services to make sure they are available to users and briefly introduces two software tools that can be used for monitoring. The second module covers the importance of firewalls and provides instructions for their configuration and deployment. The third module presents the many tasks involved in using an intrusion detection system (IDS) on a network. Topics covered include implementing IDSs on host computers and on networks, using Snort (the most common open-source IDS), and interpreting and using the information gathered using an IDS. The fourth and final module covers real-world skills and techniques for synchronizing the time on networked computers from a central clock, collecting and securing information for forensic analysis, and using a remote, centralized storage point for log data gathered from multiple computers.

ACCESSION NUMBER: ADA443478

http://handle.dtic.mil/100.2/ADA443478

Miller, Scot. ***Evaluation of Information Assurance Requirements in a Net-Centric Army.*** Carlisle Barracks, PA: Army War College, 2005. 31p.

Abstract: Network centric capabilities are a key enabler for the transformational army and planned employment of Units of Action in the future. Information Assurance refers to the security and assurance of the information that is being passed within the myriad networked systems at multiple data rates and security classifications. This paper will examine the requirements and concurrent capabilities necessary for this key strategic imperative of future Army operations as part of a joint and coalition force.

ACCESSION NUMBER: ADA432792

http://handle.dtic.mil/100.2/ADA432792

Muncaster, G. and E. J. Krall. “An Enterprise View of Defensive Information Assurance.” p. 714-718, IN: ***IEEE Military Communications Conference Proceedings, 1999***. MILCOM 1999. 1499p.

Abstract: Real-world network-centric military and commercial systems which operate within the global mixed wireless and wireline infrastructure require practical enterprise-wide defensive information assurance (DIA). The increasing reliance on common, open standards and intrinsic complexity make such systems attractive and vulnerable to information warfare attack. A proactive, enterprise-wide DIA program is prudent, given the nature of information attack threats, and is beneficial to enterprises and their global customers.

Nanton, Ulmont C., Jr. ***Achieving Information Assurance.*** Carlisle Barracks, PA: Army War College, 2004. 51p.

Abstract: Achieving Information Assurance (IA) is an integral factor in the U.S. efforts to strengthen America's homeland security. Technology enhancements have enabled greater efficiency in our business processes. At the same time we have increased our dependency on technology and thus our vulnerability. While our enemy continues to exploit conventional means to harm us in our homeland the threat of compromised information systems in critical infrastructure poses an even greater threat to our national security. Technology enables attacks against our way of life from abroad. It is no longer necessary to take the fight to your neighbor. Our inability to secure the very systems that we have become wholly dependent on could very well be the catalyst that exploits our weakness. Information assurance is the application of controls to mitigate the risk of exposure of our information systems. Our current method of dealing with information security is one of reaction. This process is in urgent need of replacement with a system of proactive protection and immediate/automated corrective action. This paper will show that near real time information assurance is achievable.

ACCESSION NUMBER: ADA424379

http://handle.dtic.mil/100.2/ADA424379

Ogren, Joel G. and James R. Langevin. ***Responding to the Threat of Cyberterrorism Through Information Assurance***. Monterey, CA: Naval Postgraduate School, June 1999. 90p.

Abstract: The number of people connecting to the Internet is growing at an astounding rate: estimates range from 100% to 400% annually over the next five years. This unprecedented level of interconnectedness has brought with it the specter of a new threat: cyberterrorism. This thesis examines the impact of this threat on the critical infrastructure of the United States, specifically focusing on Department of Defense issues and the National Information Infrastructure (NII). A working definition for cyberterrorism is derived, and a description of the Nation's critical infrastructure is provided. A number of possible measures for countering the threat of cyberterrorism are discussed, with particular attention given to the concept of information assurance. Information assurance demands that trustworthy systems be developed from untrustworthy components within power generation systems, banking, transportation, emergency services, and telecommunications. The importance of vulnerability testing (or red teaming) is emphasized as part of the concept of information assurance. To support this, a cyberterrorist red team was formed to participate in the Marine Corps' Urban Warrior Experiment. The objective of this thesis is to address the impact of these issues from a Systems Management perspective. This includes taking into account the changes that must occur in order to improve the U.S.' ability to detect, protect against, contain, neutralize, mitigate the effects of and recover from attacks on the Nation's Critical Infrastructure.

ACCESSION NUMBER: ADA366792

http://handle.dtic.mil/100.2/ADA366792

Powers, Hampton and Milica Barjaktarovic. ***Concurrent Information Assurance Architecture.*** Freeville, NY: Wetstone Technologies, Inc., 2002. 104p.

Abstract: Currently, many tasks in the information security field are accomplished in a sequential manner, often after the fact, which limits the urgency of time response and usefulness of the tools and approaches currently available. The next step toward more secure networking is taking a Concurrent Information Assurance (C-IA) approach, which executes security-critical functionality concurrently on several different levels. The C-IA Architecture (C-IAA) postulates concurrent information assurance (IA) by providing configurable, coordinated, automated situation analysis, decision assistance, and response. The C-IAA's objective is to create the underpinnings for an architecture that executes security-critical functionality in an automated fashion, distributively, concurrently, and separately from other applications. C-IAA systems exploit the severability of concurrent processing into separate execution environments to achieve a high confidence and minimal impact on information, IA components, and the organizations dependant on that information.

ACCESSION NUMBER: ADA406860

http://handle.dtic.mil/100.2/ADA406860

Scott, Kelvin B. ***An Analysis of Factors that have Influenced the Evolution of Information Assurance from World War I Through Vietnam to the Present***. Wright Patterson AFB, OH: Air Force Institute of Technology, School of Engineering and Management, 2004. 84p.

Abstract: This study is an exploratory historical analysis of the factors that have influenced the evolution of military Information Assurance (IA) programs from World War I to the present. Although the term IA has recently been widely used throughout the Information Resource Management field (IRM), evidence indicates that information and information systems protection mechanisms were used during every U.S. Military conflict. This research proposes to increase the body of knowledge within the information systems management field by exploring the areas related to Information Assurance (IA) and the ultimate goal of U. S. Defensive Information Warfare. I found that significant events related to the protection of information and information systems security led to certain levels of IA being explored throughout each U.S. Military conflict. The evaluation of these events provides key information that reveals a common approach to IA throughout history and supports the identification of key concepts that have influenced this evolutionary

process and shaped the role of IA in current military operations, with indicators of how it may be used in the future.

ACCESSION NUMBER: ADA425253

http://handle.dtic.mil/100.2/ADA425253

Sledge, Carol A. ***Building Information Assurance Educational Capacity: Pilot Efforts to Date.*** Pittsburgh, PA: Carnegie-Mellon University, 2005. 36p.

Abstract: This report describes efforts by the Software Engineering Institute (SEI) to increase the capacity of institutions of higher education to offer information assurance (IA) and information security (IS) courses, to expand existing IA and IS offerings, and to include IA and IS topics and perspectives, as appropriate, in other courses. Naturally, these efforts must be aligned with a department's foci, its current curriculum, and its accreditation requirements. To accomplish its goals, the SEI transitions courseware, materials, and a survivability and information assurance curriculum to various departments at institutions of higher education, participates in NSF-funded faculty capacity-building programs, creates partnerships with key regional educational institutions, and offers IA symposia, among other efforts. While the SEI works with all institutions of higher education, there is a particular focus on minority-serving institutions (MSIs) and community colleges in the United States. Rather than build a new infrastructure to accomplish this, the SEI utilizes partnerships that leverage the strengths of the SEI and the strengths of the partner educational institutions, builds upon existing trusted relationships and infrastructure, and sustains the incorporation of new and evolving materials. Leveraging other complementary programs, events, and organizations broadens the offering and makes it more cost effective to all parties concerned. Over the past 3 years, the SEI has developed a multi-pronged approach for its educational outreach in information assurance, with the goal of increasing the educational information assurance capacity. While the focus is primarily on information security and information assurance, the SEI also includes related software engineering areas (e.g., process improvement) that are areas of core competency for the SEI and for which the SEI offers workshops for faculty and others.

ACCESSION NUMBER: ADA441832

http://handle.dtic.mil/100.2/ADA441832

VanPutte, Michael A. **A Computational Model and Multi-Agent Simulation for Information Assurance**. Monterey, CA: Naval Postgraduate School, 2002. 178p.

Abstract: This dissertation introduces a computational model of IA called the Social-Technical Information Assurance Model (STIAM). STIAM models organizations, information infrastructures, and human actors as a complex adaptive system. STIAM provides a structured approach to express organizational IA issues and a graphical notation for depicting the elements and interactions. The model can be implemented in a computational system to discover possible adaptive behavior in an IA environment. A multi-agent simulation is presented that introduces several innovations in multi-agent systems including iconnectors, a biologically inspired visual language and mechanism for inter-agent communications. The computational model and simulation demonstrate how complex societies of autonomous entities interact. STIAM can be implemented as a hypothesis generator for scenario development in computer network defensive mechanisms.

ACCESSION NUMBER: ADA406072

http://handle.dtic.mil/100.2/ADA406072

http://bosun.nps.edu/uhtbin/hyperion-image.exe/02Jun%5FVanPutte%5FPhD.pdf

Witten, Brian. ***Information Assurance and Survivability Operational Experimentation (OPX).*** Arlington, VA: Defense Advanced Research Projects Agency, 2002. 17p.

Abstract: This briefing was presented during the Phoenix Challenge 2002 Conference and Warfighter Day. It concerns information assurance and survivability operational experimentation (OPX). The strategy of OPX objectives are to: accelerate transition of effective technologies, information research agenda with operational experience. Its key experimentation risks and transition metrics are: limited operational staff

time, and impact on operational systems. Its approach is: leverage mature research, well tested in lab, and to field cautiously.

ACCESSION NUMBER: ADA406361

http://handle.dtic.mil/100.2/ADA406361

Woodhouse, Allen F. ***Information Assurance: A National Policy Struggling With Implementation.*** Carlisle Barracks, PA: Army War College, 2001. 27p.

Abstract: *The President's Commission on Critical Infrastructure Protection was the first national effort to address the vulnerabilities created by the revolution in information technology. The Commission was established in July 1996 and rendered its report in October 1997. The results of the report were alarming. The nation's critical infrastructures had become increasingly automated, interlinked, and relied heavily on computer controlled systems. Moreover, the Commission found a wide spectrum of threats, increasing vulnerabilities in both private sector and government systems, and no national focus or policy. After reviewing the report, President Clinton issued Presidential Decision Directive 63 (PDD 63), which became the national policy for Critical Infrastructure Protection, and Information Assurance. This paper will examine the adequacy and effectiveness of PDD 63. It will focus on how clearly the policy states objectives and acceptable risks. It will address the policy's consistency with the National Security Strategy. Since more than 90 percent of the information systems that the government uses belong to the private sector, the paper will examine the private sector's role in the policy's implementation. Finally, with the current trend toward economic globalization, the issue of foreign policy cooperation must be addressed as well.*

ACCESSION NUMBER: ADA390580

http://handle.dtic.mil/100.2/ADA390580

Information Dominance

Books

Alberts, David S. and Richard E. Hayes. “The Realm of Information Dominance: Beyond Information Warfare.” p. 560-565, IN: **Proceedings of the First International Symposium on Command and Control Research and Technology.** Washington, DC: National Defense University, 19-22 June 1995. Washington, DC: National Defense University, 1996. 600p.
DKL UB212 .I573 GENERAL

Bray, Johnny W. **Information Dominance - Can We Afford It?** Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 36p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1123

Kaminski, Paul G. **Information Dominance for the Warfighter: The Present to Year 2025**. Washington, DC: Undersecretary of Defense for Acquisition and Technology. March 1998, 8p. [speech at the AFCEA Info Tech Conference, 1996, Dayton OH.]
http://www.acq.osd.mil/ousda/kaminski/info_dominance.html

Lee, James G. **Counterspace Operations for Information Dominance**. Maxwell Air Force Base, AL: Air University Press, [1994] 43p.
http://handle.dtic.mil/100.2/ADA361117

Sullivan, Shannon M. **An Air Force Command and Control Battlelab…Key to Information Dominance.** Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 35p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1086

Periodicals

Arquilla, John. "Strategic Implications of Information Dominance." **Strategic Review**, Summer 1994, v. 22, no. 3, p. 24-30.

Bey, Christopher S. “Chasing Our Tail: The Quest and the Costs for Information Dominance.” **Marine Corps Gazette**, October 1998, v. 82, no. 10, p. 18-20.

Brohm, Gerard P. “C4IEWS (Command, Control, Communications, Computers, Intelligence, Electronic Warfare and Sensors): The Enabler of Information Dominance.” **Military Technology**, May 1998, v. 22, no. 5, p. 7-9+

Brown, Scott M. “What About Information Dominance Warfare?” **Communications of the ACM**, October 1999, v. 42, no. 10, p. 13-14.

Evans, Bill. “Conservative Heavy Division: A Signal Perspective.” **Army Communicator**, Summer 1998, v. 23, no. 3, p. 11-12.

“Force XXI, ‘Philosophy, Vision and Strategy.’” **Army Communicator**, Summer 1997, v. 22, no. 3, p. 2-4.

“The Future: Two Different Views.” **Air Force Times**, May 12, 1997, v. 57, no. 41, p. 29.

Grange, David L. and James A. Kelley. "Victory Through Information Dominance." **Army**, March 1997, v. 47, no. 3, p. 32-37.

Green, Gerald. “JCS Joint Vision 2010 “I” Plan Emphasizes Information Dominance.’” **Journal of Electronic Defense**, January 1997, v. 20, no. 1, p. 19.

Gourley, Scott R. “Army Electronics and Information Dominance.” **Army**, June 1999, v. 49, no. 6, p. 41-44.

Guenther, Otto J. "Managing the Race for Information Dominance." **Army**, June 1997, v. 47, no 6, p. 23-25.

Harris, III, James E. “To Fight Digitized or Analog.” **Military Review**, November/December 1999, v. 79, no. 6, p. 12-17.

”Information Dominance Edges Toward New Conflict Frontier.” **Signal**, August 1994, v. 48, no. 12, p. 37-40.

Jones, Harry E., II. “Information Dominance for Army XXI: Battlefield Visualization.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 8-10.

Lockwood, Jonathan. “Lessons of the Winter Wargame.” **Army Times**, March 19, 1997, v. 57, no. 33, p. 54.

Libicki, Martin C. “Information Dominance.” **Strategic Forum**, November 1997, no. 132. *http://www.ndu.edu/inss/strforum/SF132/forum132.html*

Mann, Edward. “Desert Storm: The First Information War?” **Airpower Journal**, Winter 1994, v. 8, no. 4, p. 4-13. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj94/win94/man1.html*

Meadows, Sandra I. “Information Dominance Anchors Vision of Joint Warfare in 2010.” **National Defense**, December 1996, v. 81, no. 523, p. 12-13.

Minihan, Kenneth A. “Information Dominance: Meeting the Intelligence Needs of the 21st Century.” **American Intelligence Journal**, Spring-Summer 1994, v. 15, p. 15-19.

Minihan, Kenneth A. “Information Dominance: Winning in the New Dimension of Warfare.” **Spokesman**, October 1994, v. 34, no. 9, p. 10-12.

Mowery, Beverly P. “Information Determines the Battlespace as World Changes Camouflage Threats.” **Signal**, April 1996, v. 50, no. 8, p. 65-69.

Naylor, Sean D. “Hidden Soft Spot in Satellite Might.” **Army Times**, March 10, 1997, v. 57, no. 33, p. 20-21.

_____. “War Game Illustrates Vulnerabilities.” **Navy Times**, March 17, 1997, v. 46, no. 24, p. 31.

Nifong, Michael R. “The Key to Information Dominance.” **Military Review**, May/June 1996, v. 76, no. 3, p. 62-67.

Noonan, Robert W., Jr. “Army Intelligence: Achieving Information Dominance.” **Army**, October 2001, v. 51, no. 10, p. 133-134+

Peterson, Robert A. “Evolution FM 34-40 to IEW Support to C2W.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 52-53.

Robinson, Clarence A., Jr. “Information Dominance Glitters Among Commercial Capabilities.” **Signal**, June 1998, v. 52, no. 10, p. 35-39.

Scott, William B. “U.S. Deploys Advances Satcom in Bosnia.” **Aviation Week & Space Technology**, May 13, 1996, v. 144, no. 20, p. 55+

Stevens, Halbert F. “Information Dominance: The New High Ground.” **Defense Intelligence Journal**, Spring 1996, v. 5, no.1, p.43-52.

Thomas, Charles W. “Information Dominance.” **Military Intelligence Professional Bulletin**, January-March 1997, v. 23, no. 1, p. 2-3.

Wegner, Neal J. “The Intel XXXI Concept II: The Operational Patterns.” **Military Intelligence Professional Bulletin**, July-September 1996, v. 22, no. 3, p. 53-55.

Welch, Larry D. “Dominating the Battlefield (Battlespace).” **Journal of Electronic Defense**, January 1997, Supplement, p. 10-14.

Zimm, Alan D. “Human-Centric Warfare.” **United States Naval Institute Proceedings**, May 1999, v. 125, no. 5, p. 28-31.

Documents, Theses & Technical Reports

Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography.

Byram, Judith K. and James P. Harris. ***Developing and Fielding Information Dominance.*** San Diego, CA: Space and Naval Warfare Systems Center, 2002. 17p.

Abstract: This paper describes the process improvements that comprise the Space and Naval Warfare Systems Command's Horizontal Integration Initiative. It tells how these process improvements are leading to improved C4ISR capability, sustainability, and cost effectiveness as the System Command fields successive Blocks of its horizontally integrated product line: "IT-21". The process improvements represent a holistic view of end to end capabilities: commonality in hardware, software, and data structure; tight configuration management; built in ILS; and rigorous testing to horizontally integrate shipboard C4ISR designs. The paper recounts how these improvements became the foundation for SPAWAR's IT-21 re-engineering initiative; and discusses development and fielding plans for the Fleet's first fully integrated C4ISR architecture: IT-21 - Block 1. An organizational overview of the IT-21 Block 1 architecture, within its functional enclaves (GENSER, SCI, UNCLAS, Networks, Transport), lists key features of the end to end design package. As Block 1 readies for delivery in 2003, development of its successor architecture, IT-21 Block 2, is already underway. The features of the IT-21 Block 2 design process - requirements analysis, technology insertion, interface planning, and cost/benefit analysis - provide insight into the dynamics which will shape Navy C4ISR in years to come.

ACCESSION NUMBER: ADA461923

http://handle.dtic.mil/100.2/ADA461923

Catudal, Joseph T. ***Road to Information Dominance: 'System of Systems' Concept for the United States Armed Forces***. Carlisle Barracks, PA: Army War College, April 1998. 145p.

Abstract: Information and technical superiority is the foundation on which our National Military Strategy implementation rests. The advancement of technology transformed warfare into the art of employing integrated advanced information and weapons systems with forces to dominate an opponent strategically, operationally and tactically. The dominance exhibited by U.S. forces in Operation Desert Storm demonstrates reliance on advanced technology to win decisively. Maintaining a technological edge grows increasingly important as force structure decreases and high-tech smart, expert and possibly brilliant weapons become readily available on the open market. Our current technological advantage is based on past experience with an investment in technology. It is prudent and reasonable to assume that our future war fighting capabilities will be appreciably forged by today's contribution. This study focuses on information dominance through the U.S. Armed Forces System of Systems concept. It addresses and analyzes current and future strategic implications and requirements for U.S. warfighting communications and information systems. It proposes a more flexible, reliable, responsive, robust and survivable high capacity throughput communications and bitways system to support future force projection operations for the Force and/or Army After Next. Lastly, it concludes with a suggested methodology to implement the System of Systems concept to enable information dominance.

ACCESSION NUMBER: ADA343508

http://handle.dtic.mil/100.2/ADA343508

Cross, Frederick A. ***Making the Information Manager (G6/J6): Leveraging Information Management to Achieve Information Dominance.*** Carlisle Barracks, PA: Army War College, 2002. 33p.

Abstract: The three primary communications disciplines offered to signal officers by the U.S. Army Signal Corps separately do not meet the educational and training needs required of the G6/J6 Information Manager to support future doctrine. In that context, should the U.S. Army Signal School's institutional training and educational programs for its three primary officer disciplines; Basic Branch 25, Functional Area 24 and Functional Area 53, be restructured in order to provide signal officers the proper tools necessary to become an effective G6/J6 Information Manager; supporting the complex and vast informational requirements of the future warfighter? The Army Signal Corps face tremendous challenges in educating, training and aligning the proper skill-sets required of its officers to successfully assist the Army and the joint community in meeting Joint Vision 2020 objectives in information technology. Developing effective, confident and skilled Army Information Managers is essential in ensuring not only Army, but Joint warfighters as well achieve and enjoy information dominance across the entire spectrum of conflict. In the draft version of the new FM 6.0, Command and Control, the Army's information management function is assigned to the G6 (Army Signal Officer). To properly fulfill the roles and functions of the G6/J6, it is my belief that Signal Officers must be trained and educated in a cross-section of skills pulled from each of the three specific signal disciplines. The future G6/J6 Information Manager must be multi-talented, skilled and educated not only in the installation, operation and maintenance of traditional communications systems, but also proficient in tactical operations, intelligence and information systems technologies- including data network engineering and computer network and system design.

ACCESSION NUMBER: ADA400753

http://handle.dtic.mil/100.2/ADA400753

Bolstad, Cheryl A and Mica R. Endsley. ***Information Dissonance, Shared Mental Models and Shared Displays: An Empirical Evaluation of Information Dominance Techniques.*** Dayton, OH: Logicon Technical Services, Inc., 1998. 51p.

Abstract: This study experimentally tested the use of shared mental models and shared displays as a means of enhancing team situation awareness (SA). Teams were tested using a simulation of an aircraft defense task that incorporated features of a distributed team architecture. As hypothesized, the presence of shared displays and shared mental models improved team performance. However, the mechanism whereby the shared displays aided performance was not direct as expected. Teams were initially slower when first given a shared display, but a residual effect was seen in later trials where it aided performance. While shared displays initially slowed team performance in this task, most likely due to extra attention demands, they also provided for the development of shared mental models that greatly enhanced performance after they were removed. The combination of non-shared displays and no mental model was highly detrimental to performance. Teams who experienced this condition first were unable to ever develop very good performance. Overall, we found that effective team performance could be enhanced by providing teams with sufficient information to build a shared mental model of each other's tasks and goals, either through direct instruction, or through provision of shared displays.

ACCESSION NUMBER: ADA37133

http://handle.dtic.mil/100.2/ADA37133

Kaminski, Paul C. ***Information Dominance for the Warfighter: The Present to Year 2025***. Arlington, VA: Joint Publications Research Service, October 1996. 9p.

Abstract: In summary, it is clear that we encounter some difficult challenges as well as some significant opportunities as we enter the next century. Our combat forces will increasingly exploit our information dominance to turn inside an adversary's decision cycle. System of systems architectures will provide this kind of information superiority and will dominate the 21st century battlefield. In this environment, the United States will need to extend an information umbrella over our friends and allies during coalition operations. Reliance on large system of systems architectures will expose our forces to significant vulnerabilities. The traditional approach, providing a wall around our systems, will not be fully effective

against information warfare attacks. Our systems must be robust and continue adequate performance of critical services even after attacks have taken place. To design survivability into our information systems, it is my sense that perhaps we will have to take a broader view and perhaps benefit from understanding how living organisms, populations and societies survive. Information survivability or defensive information warfare is not just a DoD issue. It is a national issue. It is a concern of both public and private institutions. My sense is that there is a tremendous opportunity to leverage investment through cooperative development of dual use technologies. In a famous 1837 lecture, Ralph Waldo Emerson asked his audience, If there is any period one would desire to be born in, is it not the age of revolution, when the old and new stand side by side... Like Emerson, we, too, live in age of revolution the continuing explosion of information systems raises rich new possibilities as well as some important new vulnerabilities.
ACCESSION NUMBER: ADA340223
http://handle.dtic.mil/100.2/ADA340223

Kaura, Mary A. ***In Support of Information Dominance: Acquisitions and Organizations***. Carlisle Barracks, PA: Army War College, April 1998. 46p.
Abstract: The purpose of this work is to provide a basis and a framework for today's command, control, computer, communications, and intelligence (C4I) acquisition policies that will ensure the military is positioned to support success on the 21st century battlefield. This paper establishes an approximation of future warfare and the changing nature of organizational structures by summarizing current published works. Resulting tenets for C4I operations are then developed. A summary of the technical constraints that are related to and important for the implementation of the C4I tenets are provided. Specifically considered are technology hurdles in bandwidth, computer technology, and software complexity. Finally, current and recommended acquisition policies that are applicable to the success of C4I architectures in support of 21st century Warfare are discussed.
ACCESSION NUMBER: ADA351075
http://handle.dtic.mil/100.2/ADA351075

Kaye, Tom and George Galdorisi. ***Achieving Information Dominance: Seven Imperatives for Success.*** San Diego, CA: Space and Naval Warfare Systems Center, 2002. 22p.
Abstract: The importance of C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) as a key enabler for warfighting success has long been recognized. What has been less clear is a means for U.S.-led joint and coalition forces to achieve C4ISR dominance. Understanding not just the operational needs and the technical requirements - but also the functional capabilities required to achieve this goal - can hasten the day when C4ISR dominance for United States military forces is more than a futuristic goal. We address a critical issue - how does the technical community achieve this goal? The overarching thesis of this paper is that in order to achieve C4ISR dominance, the technical community should neither chase means to overcome extant enemy operational capabilities nor attempt to push systems to the operational forces based solely on available technology. Rather, it should build to a discrete set of functional capabilities to achieve this C4ISR dominance. This paper identifies seven functional imperatives to achieve this C4ISR dominance over an adversary. We conclude that what has remained timeless from the days of Sun Tzu to today's conflicts are the universal needs of warfighters to have the right information, at the right place, at the right time.
ACCESSION NUMBER: ADA461794
http://handle.dtic.mil/100.2/ADA461794

Kearney, Kevin N. ***Denial and Deception--Network-Centric Challenge***. Newport, RI: Naval War College, February 1999. 24p.
Abstract: Adversarial denial and deception (D&D) poses a serious challenge to future operational concepts based on perceived informational superiority. An analysis of how D&D may interact in a future network centric environment demonstrates some inherent vulnerabilities of information technology (IT) based warfighting theory. Operational D&D has continued to keep pace with sensor development and

through physical, technical and administrative means will be able to influence sensor derived information. Once our information is tainted, network centric's reliance on information dominance will become a vulnerability. Deception will travel at high speeds and effect multiple operational levels due to the networked operational picture provided by network centric theory. Our dependence on reliable and timely information, if affected by D&D, may lead to ambiguity, misdirection, and/or false security. Network centric's speed of command will further exasperate D&D's effect by increasing the speed of deception while simultaneously reducing the likely identification of deception through analysis. Our speed and networked precision may also finely hone our operational art to the point of making us predictable and therefore more susceptible to adversarial D&D. The additional network centric attributes of self synchronization, platform reduction, and adversarial lock out will also contribute to our vulnerability to D&D by creating an environment of enemy underestimation and increasing the severity of consequences of friendly action taken under the influence of adversarial D&D. The D&D challenge that network centric warfighting faces can be addressed through an increased emphasis on the importance of networked analysis. Additionally, future doctrine must reflect a clear understanding of anti-D&D methodologies so that operational commanders of the future are aware of and can plan how to counter D&D when they face it.

ACCESSION NUMBER: ADA363099

http://handle.dtic.mil/100.2/ADA363099

Lee, James D. ***Information Dominance in Military Decision Making***. Fort Leavenworth, KS: Army Command and General Staff College, June 1999. 134p.

Abstract: This study considers how ABCS (Army Battle Command System) capabilities achieve information dominance and how they influence the military decision making process. The work examines how ABCS enables commanders and staffs to achieve information dominance at the brigade and battalion levels. Further, it describes how ABCS influence battle command in an expanded battlespace. A review of recent trends at the Combat Training Centers (CTCs) indicates that no great advantage if gained is realized by achieving situational awareness at the brigade level. It appears the better-trained force in execution wins on the battlefield regardless of increased awareness. The study determined that technologies like ABCS are the first step towards producing future digitized systems that will gain information dominance for the future commander. It promotes the continued development information dominance technologies that enable a better decision-making process. It further concludes that man and battle command remain the continuity that provides ABCS its power by leveraging its capabilities at the right point and time on the battlefield. Finally, with the expanded battlespace, it identifies the problem that brigades do not have the weapons systems to influence this battlespace, hence, the current failures at the CTCs today.

ACCESSION NUMBER: ADA367899

http://handle.dtic.mil/100.2/ADA367899

Lee, James G. ***Counterspace Operations for Information Dominance.*** Maxwell AFB, AL: Air University, School of Advanced Airpower Studies, 1999. 46p.

Abstract: The launch of the Soviet "Sputnik" satellite in October 1957 shocked the world and propelled the rhetoric and the realities of the Cold War into the space age. At the same time, the Soviet feat raised the threat of mass destruction from space, and served as the basis for strategists to argue for a means to shoot down enemy satellites. Although the arguments used to justify the need for an antisatellite (ASAT) weapon have changed in the years since "Sputnik," the policy and strategy for its employment have always focused on the need to destroy, or threaten to destroy, Soviet satellites on orbit.

ACCESSION NUMBER: ADA361117

http://handle.dtic.mil/100.2/ADA361117

Lynam, D. A. ***In Search of the Holy Grail Information Dominance.*** London, UK: Ministry of Defence, 2001. 13p.

Abstract: These viewgraphs discuss information dominance which is the ability to use information to decide and act faster than the enemy while denying them the opportunity to do the same.

ACCESSION NUMBER: ADA406922

http://handle.dtic.mil/100.2/ADA406922

Mitre Corporation. ***Horizontal Integration: Broader Access Models for Realizing Information Dominance.*** McLean, VA: Mitre Corporation, Jason Program Office, 2004. 61p.

Abstract: Horizontal integration refers to the desired end-state where intelligence of all kinds flows rapidly and seamlessly to the warfighter, and enables information dominance warfare.

ACCESSION NUMBER: ADA429342

http://handle.dtic.mil/100.2/ADA429342

Murray, William P. ***'Will the Blind Be Leading the Blind,' the Clipper Chip Controversy and Its Relevance to Informational Dominance of the Battlefield***. Carlisle Barracks, PA: Army War College, 1998. 28p.

Abstract: During the 20th Century the bulk of cryptography research and use was controlled by the military. On April 16, 1993 the Clinton administration announced that the NSA had secretly developed a stronger algorithm to be integrated into a chip called 'Clipper'. The catch, however, was that the keys for the chip would remain in the hands of the U.S. government. This paper will focus on U.S. assumptions that we can control the flow of these technologies. It will examine the debate around the Clipper chip and its 'key escrow' requirements. By reviewing risk assessment, manageability and costs for this structure, one can readily view the scope and complexity of this particular government position. The speed of technological change, driven by global market forces, is bypassing our abilities to control the development of encryption products. This change will challenge our basic concepts of informational dominance of the battlefield as envisioned in Department of Defense's Revolution in Military Affairs (RMA) paradigm. Global demand for encryption devices is growing quickly. The United States is being faced with a choice; adapt to the market imperatives, which must include revising our RMA viewpoints, or be left behind and face the inevitable consequences both economically and militarily.

ACCESSION NUMBER: ADA351146

http://handle.dtic.mil/100.2/ADA351146

Neal, William J., et al. ***Battlefield Visualization***. Washington, DC: Army Science Board, December 1998. 121p.

Abstract: A study analyzing battlefield visualization (BV) as a component of information dominance and superiority. This study outlines basic requirements for effective BV in terms of terrain data, information systems (synthetic environment; COA development and analysis tools) and BV development management, with a focus on technology insertion strategies. This study also reports on existing BV systems and provides 16 recommendations for Army BV support efforts, including interested organization, funding levels and duration of effort for each recommended action.

ACCESSION NUMBER: ADA363997

http://handle.dtic.mil/100.2/ADA363997

Oltman, Charles B., et al. ***Interdiction: Shaping Things to Come***. Maxwell AFB, AL: Air University, Air Command and Staff College, 1996. 43p.

Abstract: Interdiction, based on the core competencies of precision employment and information dominance will still be used to shape the battlespace in 2025. The critical pieces of these core competencies - accuracy, lethality, target identification, and cycle time - will necessarily undergo great

change in the next 30 years. The result of these changes will be interdiction with a different face but the same heart. Interdiction in 2025 will require affordable enhancements to current capabilities in the areas of accuracy, lethality, target detection/identification, and timeliness, allowing the war fighter to shape the battlespace in revolutionary ways. A number of technological "leaps" will drive these required changes. Penetrating sensors and designators, coupled with microtechnology, will permit weapons to have the processing power required to "touch" targets in exactly the right spot. Variable lethality will permit the option of killing, delaying, deterring, or breaking targets. Synergistically combining these capabilities with intelligent system logic processing, improved target detection, decreased sensor-to-weapon cycle time, and air power will provide the necessary pieces to dominate the battlespace. Among the systems required to build the interdiction system of systems in 2025 are: beyond- electromagnetic sensors; acoustic, penetrating, and variable-yield weapons; sensory netting; energy and particle weapons; and a virtual observe, orient, decide, and act (OODA) loop. From these systems, a nexus of three enabling technologies emerges. If pursued, these technologies will provide the leveraged investment necessary to revolutionize interdiction.

ACCESSION NUMBER: ADA332935

http://csat.au.af.mil/2025/volume3/vol3ch05.pdf

http://handle.dtic.mil/100.2/ADA332935

Orr, Joseph E. ***Information Dominance: A Policy of Selective Engagement***. Carlisle Barracks, PA: Army War College, April 1997. 27p.

Abstract: 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 examines information as an instrument of national power; argues the need for a national information strategy; highlights the risks associated with a growing dependence on information; and discusses the need for new guidelines, laws, and agreements to govern cyberspace.

ACCESSION NUMBER: ADA326787

http://handle.dtic.mil/100.2/ADA326787

Perusich, Karl and Michael D. McNeese. ***Understanding and Modeling Information Dominance in Battle Management: Applications of Fuzzy Cognitive Maps***. West Lafayette, IN: Purdue University, March 1998. 98p.

Abstract: The report takes a unique look at information dominance and how it relates to shared situation awareness and the decision making cycles of the OODA loop. An explanation of information dominance is developed through a historical example of battle management (the Battle of Britain) to demonstrate the various levels of information interconnectivity. This example is then extrapolated to look at the constraints and options existent within contemporary information dominance. Fuzzy cognitive mapping, a method for eliciting and modeling human interactions in complex situations (such as information dominance) is introduced and applied to a real world scenario. The role of fuzzy cognitive maps: (1) as a means to explicate cause effect relationships in individual and teamwork settings; and (2) to model emergent complexity in information dominance situations; is described using the context of the real world scenario. The use of fuzzy cognitive maps is reviewed and evaluated for effectively capturing and abstracting knowledge relevant to shared situation awareness.

REPORT NUMBER: AFRLHE-WP-TR-1998-0040

ACCESSION NUMBER: ADA352913

http://handle.dtic.mil/100.2/ADA352913

Reeves, Brian. ***General Matthew B. Ridgway: Attributes of Battle Command and Decision-Making***. Newport, RI: Naval War College, Joint Military Operations Department, February 1998. 23p.

Abstract: What affect will information superiority have on the decision-making process of the future. Will information dominance require the attributes of future battle commanders be different than those of the past. This paper focuses on the intellectual and personality traits of General Matthew B. Ridgway as they apply to operational command and decision-making. These traits are considered essential for analysis and serve as a framework in which to examine their applicability to future command. The essential qualities of an operational commander are divided into two categories: intellect and personality. Each category is further divided into elemental traits. The application of these traits to Ridgway as they pertain to his command in the Korean war serve to demonstrate their permanence.

ACCESSION NUMBER: ADA348394

http://handle.dtic.mil/100.2/ADA348394

Velasco, Diego, Jr. ***Full Spectrum Information Operations and the Information Professional Officer Intermediate Qualification Process: Filling the Gap to Ensure the Continued Leadership of the Information Professional Community in the Area of Information Dominance.*** Monterey, CA: Naval Postgraduate School, 2005. 71p.

Abstract: There currently exists a major effort within the United States Navy's Information Professional (IP) Community to overhaul and improve the qualification process for its officers. The overall effort has included the addition of technical refresher courses, re-examination of the Continuing Education Units (CEU) system, and the improvement of the Basic, Intermediate, and Advanced Qualification programs. This thesis specifically addresses the Intermediate Qualification (IQ) and the lack of Information Operations (IO) concepts therein. While some portions of the IQ that address highly technical areas exist, there is little to no mention of the importance of and concepts contained within IO, as defined by Joint Doctrine. The IP Community has a unique opportunity to train its officers in the concepts, competencies, and supporting activities of IO. This will ensure that the IP Community continues to be the Navy's leaders in the area of information dominance. This thesis provides recommended line items for injection into the IP IQ in the appropriate format with discussions and definitions that address the specific line items. The thesis also provides further recommendations for the continuing improvement and refinement of the IP qualification process, especially in the area of IO.

ACCESSION NUMBER: ADA439831

http://handle.dtic.mil/100.2/ADA439831

Viall, Kenneth E. ***Medium Brigade 2003: Can Space-Based Communications Ensure Information Dominance?*** Fort Leavenworth, KS: Army Command and General Staff College, 2000. 118p.

Abstract: This thesis analyzes space-based communications support for medium brigade combat team forces over the next three years. The army's reaction to changes in the national security environment and increased technology as outlined in Joint Vision 2010 has been to pursue digitization of the force and develop a new, Medium Weight brigade-- rapidly deployable, reliant on high-capacity information architecture, and capable of early entry and stability and support operations. The study examined the role of satellite communications in the objective command and control system that considered the nature of the higher headquarters, adjacent units, and internal brigade requirements. Using the proposed Initial Brigade Combat Team concept, the study reviewed task organization, signal support structure, bandwidth requirements, and the operational employment of satellite communications assets during Operation Restore Hope, Somalia; Operation Uphold Democracy, Haiti; and Operation Joint Endeavor, Bosnia-Hercegovina. The study concluded that space-based communications will remain pivotal to successful command and control and projected signal organizations and equipment of the medium brigade can provide effective support. However, the army must address shortfalls in national satellite infrastructure, reconcile task organization difficulties, and integrate digitization efforts to effectively manage available communications capacities.

ACCESSION NUMBER: ADA388156
http://handle.dtic.mil/100.2/ADA388156

Wentz, Larry K. and Lee W. Wagenhals. ***Integration of Information Operations into Effects-Based Operations: Some Observations.*** Fairfax, VA: George Mason University, 2003. 36p

Abstract: Information Operations (IO) has become a primary war fighting capability and is now considered a military core competency. The military Services are establishing IO as a military career field equivalent to other war fighting fields and they are developing supporting education and training programs to create a pipeline of trained and experienced information operations warriors. Transforming doctrine into an operational reality has, however, proven to be a challenge and the training programs and operational planning and assessment tools have been slow to materialize. Operations in the Balkan's and Afghanistan have afforded the military the opportunity to conduct IO and to document experiences and lessons from these real world operations. A number of experiments and exercises also have explored new military concepts that included the use of non-kinetic IO means of national power to influence adversary behavior and actions. This paper explores some of the challenges of executing and assessing IO courses of action including some observations regarding integration of IO into EBO. The insights and observations offered are based on the authors multiple experiences. Operationalizing IO is work in progress and much remains to be done to bridge policy, doctrine, applications and tools.

ACCESSION NUMBER: ADA468338
http://handle.dtic.mil/100.2/ADA468338

Whitaker, Randall D. and Gilbert G. Kuperman. ***Cognitive Engineering for Information Dominance: A Human Factors Perspective***. Dayton, OH: Logicon Technical Services, Inc., October 1996. 129p.

Abstract: Information Warfare (IW) is emerging as the critical military issue of the day. IW is introduced and analyzed with respect to its major themes and current definitions. Those aspects of IW requiring cognitive engineering research are identified, necessary methodological reorientations are outlined, and key links to the human factors/cognitive engineering topics of situation awareness and decision making are discussed. A specific target capability (the common battlespace picture) and the framework for research toward that goal (the OODA model) are introduced. The OODA model is contextualized with respect to other relevant research areas and U.S. Air Force practices. An integrated cognitive engineering program for IW analyses is specified and illustrated with respect to an example drawn from theater missile defense (TMD) attack operations. Extensive listings of bibliographic references, terminological definitions, and relevant Internet resources provide a solid foundation for further reading and research.

ACCESSION NUMBER: ADA323369
http://handle.dtic.mil/100.2/ADA323369

Information Superiority

Books

Brice, Michael D. **Strategic Surprise in an Age of Information Superiority. Is it Still Possible?** Maxwell AFB, AL: Air University, Air War College, 2003. 29p.
https://research.maxwell.af.mil/viewabstract.aspx?id=4399

Builder, Carl H., Steven C. Bankes, and Richard Nordin. **Command Concepts: A Theory Derived From the Practice of Command and Control**. Santa Monica, CA: Rand, 1999. 165p.
http://www.rand.org/pubs/monograph_reports/2006/MR775.pdf
DKL UB212 .B85 1999 GENERAL

Clements, Stacy M. **The One with the Most Information Wins? The Quest for Information Superiority**. Wright-Patterson AFB, OH: Air Force Institute of Technology, 1997. 119p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1170

Gompert, David C., Irving Lachow and Justin Perkins. **Battle-Wise: Seeking Time-Information Superiority in Networked Warfare.** Washington, DC: National University Press, Center for Technology and National Security Policy, 2006. 174p.
http://www.ndu.edu/inss/books/2007/B-W_final.pdf
DKL UB212 .G66 2006 GENERAL

Marrs, James R. **Assessing Air Force Investment and Opportunities in Information Superiority**. Maxwell AFB, AL: Air University, School of Advanced Airpower Studies, 1999. 82p.
https://research.maxwell.af.mil/viewabstract.aspx?id=2046

Matsumura, John, et al. **Joint Operations Superiority in the 21st Century: Analytic Support to the 1998 Defense Science Board**. Santa Monica, CA: Rand, 1999. 51p.
http://www.rand.org/pubs/documented_briefings/2005/DB260.pdf
DKL U260 .J565 1999 GENERAL

Perry, Walt L., David Signori, and John Boon. **Exploring Information Superiority: A Methodology for Measuring the Quality of Information and Its Impact on Shared Awareness.** Santa Monica, CA: RAND, 2003. 141p.
http://www.rand.org/pubs/monograph_reports/2005/MR1467.pdf
DKL UB212 .P47 2003 GENERAL

Proceedings of the 8th International Command and Control Research and Technology Symposium. "Track 7 Information Superiority/Information Operations." National Defense University, Washington, DC, 17-19 September 2003. Washington, DC: National Defense University, 2003.
http://www.dodccrp.org/events/2003/8th_ICCRTS/Tracks/track_7.htm

Proceedings of the 9th International Command and Control Research and Technology Symposium. "Track 8.1 Information Superiority/Information Operations." Copenhagen, Denmark, 14-16 September 2004. Washington, DC: National Defense University, 2004.
http://www.dodccrp.org/events/8th_ICCRTS/foreword.htm

Proceedings of the 2001 Command and Control Research and Technology Symposium. "Track 7 Information Superiority/Information Operations." US Naval Academy, Annapolis, MD, 19 June – 21 June 2001. Washington, DC: National Defense University, 2001.
http://www.dodccrp.org/events/6th_ICCRTS/index.htm

Proceedings of the 2002 Command and Control Research and Technology Symposium. "Track 7 IS/IO." Naval Postgraduate School, Monterey, CA, 11-13 June 2002. Washington, DC: National Defense University, 2002.
http://www.dodccrp.org/events/2002_CCRTS/fore.htm

Proceedings of the 2004 Command and Control Research and Technology Symposium. "Track 3 Information Superiority/Information Operations", San Diego, CA, 15-17 June 2004. Washington, DC: National Defense University, 2004.
http://www.dodccrp.org/events/2004_CCRTS/CD/foreword.htm

United States. General Accounting Office. **Defense Information Superiority: Progress Made, But Significant Challenges Remain**. GAO/NSIAD/AIMD-98-257. Washington, DC: The Office; Gaithersburg, MD, 1998. 28p.
http://www.gao.gov/archive/1998/n198257.pdf

Periodicals

Ackerman, Robert K. “Jointness Defines Priorities for the Defense Department's Global Grid.” **Signal**, April 2001, v. 55, no. 8, p. 23-27.

Antal, John F. “Lessons Learned from the Fighting in Afghanistan.” **Army**, June 2002, v. 52, no. 6, p. 14-16.

Barwinczak, Patricia M. “Achieving Information Superiority.” **Military Review**, September-November 1998, v. 78, no. 5, p. 36-40.

Bauer, Claude J. “Connecting in the Year 2000.” **Air Force Times**, September 14, 1998, v. 59, no. 6, p. 8-9.

Belen, Fred C. “Enabling Information Superiority in the Littoral Battlespace.” **Marine Corps Gazette**, March 1998, v. 82, no. 3, p. 15-17.

Bell, B.B. “Is Information Superiority All It's Cracked Up to Be? **Armor**, March-April 2001, v. 110, no. 2, p. 5+

Bowdish, Randall G. “Information-Age Psychological Operations.” **Military Review**, December-February 1998-1999, v. 78, no. 6, p. 29-34.

Busey, James B., IV. "Information Superiority Dashes Thorny Power Projection Issues." **Signal**, November 1994, v. 49, no. 11, p. 13+

Cardinal, Charles N. “Delivering Joint Information Superiority.” **Joint Force Quarterly**, Autumn/Winter 1999-2000, no. 23, p. 47-50.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1123.pdf

Cebrowski, Arthur K. “Sea Change [Shift From Platform-Centric to Network-Centric Warfare – Exploiting Information Superiority].” **Surface Warfare**, November/December 1997, v. 22, no. 6, p. 2-6.

Clemins, Archie R. "Information Superiority in the Pacific Fleet." **Joint Force Quarterly**, Autumn-Winter 1997-1998, no. 17, p. 67-70.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1417pgs.pdf

Covault, Craig. “Shuttle Radar Goal: Information Superiority.” **Aviation Week & Space Technology**, January 31, 2000, v. 152, no. 5, p. 38.-39.

Daembkes, Heinrich. “Network-Centric Operations and Information Superiority: Current Trends of Key Enabling Technologies.” **Microwave Journal**. (International Ed.), October 2006, v. 49, no. 10, p. 24-40.

Donskov, Yu E. and V. V. Fomin. “Information Superiority in Warfare.” **Military Thought,** 2003, v. 12, no. 4, p. 157-161.

Elliott, Ronald D. “Security Must Include Information Superiority.” **Federal Computer Week**, May 10, 1999, v. 13, no. 14, p. 19.

Fulghum, David A. “Info War Fleet Tapped For Fast Deployment.” **Aviation Week & Space Technology**, February 9, 1998, v. 148, no. 6, p. 90-91.

Garcia, Gregory L. “U.S. Air Force’s Cryptologic Systems Group: Putting the “Super” in Information Superiority.” **DISAM Journal of International Security Assistance Management**, Summer 2001, v. 23, no. 4, p. 29-33.
http://www.disam.dsca.mil/pubs/Archives/Journal23-4.pdf

Garner, Jay M. “The Next Generation of Threat to U.S. Military Superiority . . . 'Asymmetric Niche Warfare.'” **Phalanx**, March 1997, v. 30, no. 1, p. 1+

Garrett, Anthony R. “Information Superiority and the Future of Mission Orders.” **Military Review**, November/December 1999, v. 79, no. 6, p. 61-69.

Goral, Frank I. and William R. Swart. “Information Superiority: The Enabler of the Future.” **Cyber Sword**, Fall 1997, v. 1, no. 2, p. 6-9.

Hutchinson, William E. “The 'Flexibility' of Official Information During Contemporary Conflicts.” **Journal of Information Warfare,** September 2005, v. 4, no. 2, p. 38-44.

“Information and Command and Control.” **Aerospace America**, December 1999, v. 37, no. 12, p. 32-33

“Information Superiority.” **Airman**, January 1999, v. 43, no. 1, p. 10-11.

“Information Superiority.” **United States Naval Institute Proceedings**, January 1998, v. 124, no. 1, p. 30-31.

“Information Superiority Won't Win Wars By Itself.” **Aviation Week & Space Technology**, April 28, 1997, v. 146, no. 18, p. 74.

Johnstone, Mark A. and Stephen A. Ferrando. “Joint Experimentation: A Necessity for Future War.” **JFQ: Joint Force Quarterly**, Autumn 1998/Winter 1999, issue 20, p. 15-25.
http://www.dtic.mil/doctrine/jel/jfq_pubs/0620.pdf

Keeter, Hunter C. “Network Centric Warfare: Aims to Translate Information Superiority into Combat Advantage.” **Sea Power**, March 2004, v. 47, no. 3, p. 12-14.

Kuperman, Gilbert G., Scott M. Brown and Randall D. Whitaker. "Information Superiority Through Advanced Multi-Sensory Command and Control Technologies." **AFRL Technology Horizons**, June 2001, v. 2, no. 2, p. 18-19.

Langridge, Donald L. "Freedom's Sentinel in Space--The National Reconnaissance Office (NRO)." **Military Intelligence Professional Bulletin**, April-June 2002, v. 28, no. 2, p. 5-8.
http://www.universityofmilitaryintelligence.us/mipb/archives/v28n2.pdf

McDuffie, John M. "Joint Vision 2010 and Focused Logistics." **Army Logistician**, January/February 1999, v. 31, no. 1, p. 7.

Nicholson, Demetrios J. "Seeing the Other Side of the Hill": The Art of Battle Command, Decisionmaking, Uncertainty, and the Information Superiority Complex." **Military Review**, November/December 2005, v. 85, no. 6, p. 57-64.
http://usacac.army.mil/CAC/milreview/download/English/NovDec05/Nicholson.pdf

Paige, Emmett, Jr. "Striving for Information Superiority." **Defense Issues**, June 22, 1996, v. 11, no. 72, p. 1-3.
http://www.defenselink.mil/speeches/speech.aspx?speechid=1009

Parrish, Gary L. "Moving to a Digitized Center of Excellence." **Military Intelligence Professional Bulletin**, October-December 2000, v. 26, no. 4, p. 33,37+ [IS]
http://www.universityofmilitaryintelligence.us/mipb/archives/v26n4.pdf

Roberts, Terry W. "The Power of Virtual Collaboration and XML Knowledge Bases in Support of U.S. Information Superiority." **Cyber Sword**, Fall 1999, v. 3, no. 1, p. 32-34.

Robinson, Clarence A., Jr. "Information Superiority Drives Pentagon Policy and Guidance." **Signal**, July 1998, v. 52, no. 11, p. 23-27.

Smith, Bob. "The Challenge of Space Power (*)." **Airpower Journal**, Spring 1999, v. 13, no. 1, p. 32-39. [Adapted from a speech given November 1998]
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/spr99/smith.html OR
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/spr99/smith.pdf

"Targets in Cyberspace." **Military Review**, September/October 1999, v. 79, no. 5, p. 35.

Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." **Parameters**, Spring 2000, v. 30, no. 1, p. 13-29.
http://carlisle-www.army.mil/usawc/Parameters/00spring/thomas.htm

Turner, Ron "Architecting for Information Superiority." **Program Manager**, September/October 1999, v. 28, no. 5, p. 56-57.
http://www.dau.mil/pubs/pm/pmpdf99/don02so.pdf

Van Riper, Paul K. "Information Superiority." **Marine Corps Gazette**, June 1997, v. 81, no. 6, p. 54-62.

_____. "Information Superiority Won't Win Wars by Itself." **Aviation Week & Space Technology**, April 28, 1997, v. 146, no. 18, p. 74.

Wells, C. J. "Information Superiority & Support: Misplaced & Misunderstood." **Journal of Information Warfare**, March 2005, v. 4, no. 1, p. 49-60.

Wielhouwer, Peter W. "Toward Information Superiority: The Contribution of Operational Net Assessment." **Air & Space Power Journal**, Fall 2005, v. 19, no. 3, p. 85-96 *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/fal05/wielhouwer.html*

Wolffe, Jim. "'Toward the Space and Air Force.'" **Air Force Times**, May 5, 1997, v. 57, no. 40, p. 10.

Wright, Richard L. "Advantage Navy [Impact of Network-Centric Warfare -- Information Superiority]." **Surface Warfare**, November/December 1997, v. 22, no. 6, p. 7-9.

_____. "Information Superiority: Increasing the Warfighter's Advantage." **Surface Warfare**, January/February 1997, v. 22, no. 1, p. 10-13.

Documents, Theses & Technical Reports

Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography.

Blaska, Steven J. ***Achieving Information Superiority: Putting Clothes on the Emperor.*** Newport, RI: Naval War College, 2000. 33p.

Abstract: Information superiority is a critical enabler for Joint Vision 2010's Operational Concepts. Unfortunately, there are few concrete assessments that quantify where we are today and what it will take to achieve success. This paper proposes that if we analyze the components of Information Superiority in doctrinal terms, we find that one current, critical weakness is our capacity to transform data into battlespace understanding. This paper also suggests an exercise strategy that could help quantify and correct this weakness. Reality-based transformation and innovation can occur if we keep certain touchstones in mind. First, we need to make sure we communicate within a mutually understood frame of reference. Doctrine does that for u% by defining common terms and concepts. Second, even revolutionary change starts from where we stand. We can achieve successful leaps in capability as long as we are sure we do not assume away needed solutions to hard problems. An evaluation of our current capabilities shows us the toughest problem we face right now is our ability to transform data into battlefield understanding. Third, we need to test and quantify our progress in order to make sure our assumptions are still correct. The military has long used exercises accomplish this mission. We have the capability to apply this same tool to this challenge.

ACCESSION NUMBER: ADA381884

http://handle.dtic.mil/100.2/ADA381884

Brandl, Thomas. ***Information Management: The Joint Task Force's Key to Achieving Information Superiority.*** Newport, RI: Naval War College, 2000. 21p.

Abstract: Joint Vision 2010 identifies information superiority as the key enabler for decisive operations and, ultimately, full spectrum dominance. Advances in information and sensor technologies have exponentially increased the quantity of information that a JTF receives. However, simply having access to vast amounts of information does not guarantee that a JTF will achieve information superiority. The information must be properly processed and disseminated. Therefore information management (IM) is one of the most critical challenges that a JTF faces-one that it must successfully surmount in order to achieve information superiority. Despite great progress in IM training and doctrine in the past few years, IM remains a challenge to JTFs. The key to successful IM in a JTF is to develop a successful information management plan (IMP) and the commander's involvement in all aspects of IM. The IMP should contain comprehensive instructions and procedures for the collection, processing, prioritization and dissemination of information. Clearly, information management (IM) is a challenge and must be resolved in order to realize the full spectrum dominance envisioned in JV 2010.

ACCESSION NUMBER: ADA381669

http://handle.dtic.mil/100.2/ADA381669

Brice, Michael D. ***Strategic Surprise in an Age of Information Superiority: Is It Still Possible.*** Maxwell AFB, AL: Air University, 2003. 36p.

Abstract: Joint Vision 2020 asserts the United States military will achieve information superiority over any future adversary. This assertion is based on three assumptions: offensive information operations will provide an accurate and complete picture of an adversary, defensive information operations will prevent adversaries from attacking friendly information systems and the will of the US to overcome internal limitations to correctly interpret information will allow it to dominate the information realm against any opponent. However, evidence indicates these assumptions are flawed and the United States is vulnerable

to strategic surprise. In fact, according to Eliot Cohen, one might usefully call the past dozen years the age of surprises The US government has been surprised by the end of the Warsaw Pact, the disintegration of the Soviet Union, the Iraq invasion of Kuwait and the ensuing Persian Gulf War, the Asian Financial Crisis, the Indian and Pakistani nuclear detonations, and now the events of September 11, 2001. There is no reason to think the age of surprises is over, and there are many reasons to think we are still at its beginning.

ACCESSION NUMBER: ADA424856

http://handle.dtic.mil/100.2/ADA424856

Burke, Martin. ***Information Superiority, Network Centric Warfare and the Knowledge Edge.*** Salisbury, Australia: Defence Science and Technology Organisation, 2000. 23p.

Abstract: The report notes that a socio-cultural phenomenon has occurred in the Defense community whereby it is has become commonplace for the assumption to be made that success in various types of modem warfare will be assured if Information Superiority can be achieved. It presents outline arguments that suggest that this assumption is fallacious. It concludes that: Success in Network Centric Warfare requires Knowledge Superiority and benefits from Information Superiority. Success in Maneuvers Warfare requires Knowledge Superiority and benefits from Information Superiority. A Decision Edge requires a Knowledge Edge and benefits from an Information Edge.

ACCESSION NUMBER: ADA380939

http://handle.dtic.mil/100.2/ADA380939

Cardinal, Charles N. ***Delivering Joint Information Superiority.*** Washington, DC: National Defense University, Center for Counterproliferation Research, 2000. 5p.

Abstract: Joint tactical C4ISR architecture -- or the integration of command, control, communications, computers, intelligence surveillance, and reconnaissance assets -- has long been a focus of defense visionaries. They picture systems linking assets, enabling the Armed Forces to detect and strike targets with blinding speed. Such architecture has broader implications. It can enable Joint Vision 2010 and ultimately a revolution in military affairs. An advanced concept technology demonstration (ACTD) by U.S. Pacific Command (PACOM) represents progress in realizing such visionary concepts. The Under Secretary of Defense for Acquisition and Technology testified before Congress that, "We must achieve an interoperable and integrated, secure, and smart C4ISR infrastructure that encompasses both strategic and tactical needs. Enhanced situation awareness and information assurance are. . .the backbone of the revolution in military affairs." That potential was realized in part during the Persian Gulf War. U.S. forces could see targets faster with airborne warning and control and joint surveillance target attack systems. And they could hit them with greater precision. But operations are often far from perfect. The old problem remained: getting the right information to the right place at the right time. A fully integrated C4ISR architecture is the solution. It can bind the services together with defense, intelligence, and other governmental agencies. It will synchronize the unique strengths of organizations and enable the more seamless integration of service capabilities sought by JV 2010. This system of systems can link all sensors -- strategic, theater, and tactical -- within an enhanced command and control framework. Information will be fused with other friendly information and distributed as a common operational picture to users. Just as the computer and Internet have empowered individuals, shared information from an integrated C4ISR architecture may do the same for small units.

ACCESSION NUMBER: ADA426733

http://handle.dtic.mil/100.2/ADA426733

Childs, James C. ***MOOTW and Information Superiority: The Importance of Continuity As a Principle of MOOTW in the 21st Century.*** Newport, RI: Naval War College, Joint Military Operations Department, 2000. 27p.

Abstract: MOOTW encompass a wide variety of diverse missions, which are characterized by political sensitivity and less than concrete objectives. A commander may have little control over MOOTW in his

theater, yet he is ultimately responsible for the success of any missions occurring there, making coordination of all MOOTW within his theater is a formidable task. The principle of continuity, the idea that all operations, regardless of the extent of a commander's involvement in them, can be planned and coordinated toward defined objectives across the spectrum of MOOTW, is the key to success in MOOTW. Continuity will ensure that MOOTW are coordinated very much the like traditional wartime campaign plan, but with an emphasis on interagency cooperation, sharing of information and intelligence (essential when taken within the context of Joint Vision 2010 and its demand for information superiority), and the current principles of MOOTW. readiness both for increased hostilities and for post-hostility restoration. Focusing on continuity ensures readiness for all contingencies, and enables the commander to better anticipate the transition point to hostilities. In addition, as the difficulties with Operation Just Cause showed in Panama, focusing on continuity will also make planning for those operations easier and, perhaps more importantly, will ensure the proper framework is in place for transition to post-hostilities. This paper analyzes the current principles of MOOTW, drawing on MOOTW aver the past two decades and looking to the future of MOOTW and the military's role. It introduces continuity as a proposed addition to the MOOTW principles, explains its particular relevance for the future, examines counter-arguments to its adoption as a principle, and urges for a change which embraces continuity as an essential tenet of joint doctrine.

ACCESSION NUMBER: ADA378510

http://handle.dtic.mil/100.2/ADA378510

Corman, David E., et al. ***Transforming Legacy Systems to Obtain Information Superiority.*** St. Louis, MO: Boeing Co., 2001. 10p.

Abstract: *The United States and its allies are being challenged by the advantages (and threats) of the Global Information Age. In response to these challenges, a new force structure is being proposed which is built upon global awareness, global engagement, and rapid deployment of specific (effects based) forces. Revolutionary advances in information resources and technology are key contributors to this force structure. In the face of a constrained DOD budget, an unprecedented system demand for lean operations in both peacetime and wartime, and the emergence of threats requiring immediate response, it is imperative that innovative technologies be developed to enable legacy weapon systems to exploit the information revolution, achieve information dominance, and meet the required operational tempo. This paper presents an embedded-system architecture, open system middleware services, and a software wrapper schema that will enable legacy systems to fully exploit evolving information technology capabilities in the context of an Network Centric Information Architecture (NCIA).*

ACCESSION NUMBER: ADA457962

http://handle.dtic.mil/100.2/ADA457962

Dunn, III, Charles, et al. ***Information Superiority/Battle Command (Network Centric Warfare Environment)***. Fort Gordon, GA: Battle Command Laboratory, 2004. 38p.

Abstract: *The Battle Command Battle Laboratory is the U.S. Army's test bed for advanced networking and telecommunications experimentation. Over the past two years the lab has conducted a series of experiments focused on the Army's conceptual Future Force network. These experiments were designed to integrate a myriad of network-related study issues into a technical analysis of future network concepts. The results of these experiments provide the analytical underpinnings supporting the viability of transitioning the conceptual design of the Army's Future Force into an actual warfighting entity. The Army's Future Force is designed to be a faster, lighter, but more lethal force than today's force. The Future Force will use information superiority as its premier combat enabler. Information superiority coupled with an ultra-reliable networked Battle Command and Control (C2) system will ensure that separate units fight as one. This connectivity and orchestration are performed within a network-centric environment. The Army's view of Network Centric Warfare can be described as the orchestration of integrated successes of its core operational concepts (dominant maneuver, precision engagement, focused/just-in-time logistics, space-to-mud telecommunications, and full dimensional protection), which are all dependent upon information superiority.*

ACCESSION NUMBER: ADA465983

http://handle.dtic.mil/100.2/ADA465983

Ellis, Jeffrey A. ***Joint Vision 2010: Information Superiority and Its Effect on the Command and Control Process***. Newport, RI: Naval War College, Joint Military Operations Department, February 1998. 20p.

Abstract: With the implementation of Joint Vision 2010, information superiority will impact every aspect of operational art, but none will be so great as the impact on operational command and control. Through information superiority, the operational commander theoretically gains a clearer picture of the battlespace, thus mitigating the fog of war. This study examines some of the potential command and control issues facing the operational commander as he attempts to conduct Major Operations and Campaigns. Given the diverse threat, it is doubtful that U.S. forces can gain and maintain information superiority over our enemies. The need for information superiority will hamper our ability to operate in a combined environment. Information superiority may lead to operational command and control that is too rigid and too centralized to maintain friendly freedom of action. Operational commanders may become transfixed by increasing levels of information focusing on data instead of the application of forces in space and time. In the end, information superiority will provide a clearer picture of the battlespace but it will not mitigate the fog of war.

ACCESSION NUMBER: ADA348564

http://handle.dtic.mil/100.2/ADA348564

Erwin, Ralph M. ***Geospatial Information in Support of Information Superiority***. Carlisle Barracks, PA: Army War College, 2002. 34p.

Abstract: Given the proliferation of commercial imaging systems and commercially available geospatial information systems, can the National Imagery and Mapping Agency (NIMA) provide U.S. forces with the data required to achieve information superiority with respect to terrain? This is possible only if NIMA can build and provide warfighters geospatial information faster, relevant, and more accurate than any adversary, therefore achieving information dominance. An adversary will also want to see the battlespace with the same fidelity. If the same information is available to all, then the U.S. will have to determine the geospatial information preparedness level required to maintain the information edge. An information superiority edge will be sustained by adherence to NIMA established standards of timeliness, relevance, and accuracy for geospatial information. Because of the availability of geospatial information from commercial sources, adversaries of the U.S. may have an archive of readiness data that is relevant and fairly accurate, yet it appears that our adversaries will lack a responsiveness capability for timely geospatial data leaving U.S. forces with an information edge.

ACCESSION NUMBER: ADA400998

http://handle.dtic.mil/100.2/ADA400998

Hayes-Roth, Rick. ***Two Theories of Process Design for Information Superiority: Smart Pull vs. Smart Push***. Monterey, CA: Naval Postgraduate School, 2006. 39p.

Abstract: This paper examines how information should flow among networked entities in Network-Centric Operations and Warfare (NCOW). In particular, should the entities actively seek, acquire, and process relevant information, or should they wait to react to information that others send to them? In short, should they pull information, or should they rely upon others to push information to them? In most tactical contexts, "smart push" will improve efficiency by orders of magnitude compared to "smart pull." This analysis reveals that efficient information processing chains require a general capability to watch for key events. Humans and the computer applications supporting them will use this capability to detect events matching conditions of interest they specify. This capability plays a key role in transforming networks into integrated value chains. Where traditional networks aim at supporting unregulated exchanges for data bit flows best suited to random access and unpredictable process sequences, the capability to delegate condition monitoring enables one to transform networks into conveyers of timely, valuable information. To maximize efficiency, one must use processes in which each successive step receives information just as valuable as its input. Thus, condition monitoring and its associated "smart

push" constitute a required foundation for the efficient process chains needed to achieve information superiority. Seventeen briefing charts summarize the presentation.

ACCESSION NUMBER: ADA461578

http://handle.dtic.mil/100.2/ADA461578

Hogan, Todd C. ***Persistent Intelligence, Surveillance, and Reconnaissance Dilemma: Can the Department of Defense Achieve Information Superiority.*** Fort Leavenworth, KS: Army Command and Staff College, 2007. 89p.

Abstract: Joint Force commanders, military services and governmental agencies recently stated an operational requirement for a persistent intelligence, surveillance, and reconnaissance (ISR) capability. The need for persistence implies a need to detect, identify, and characterize change in a target's status anywhere, anytime, in any weather, with increasingly higher levels of fidelity. Persistent ISR is the ability to do this with sufficient timeliness and precision to achieve the Joint Force Commander's (JFC) objectives. The Global War on Terror's (GWOT) multitude of threats demands an ISR capability with the persistence to find, fix, and track single individuals in a crowd; locate camouflaged, concealed, or mobile weapons of mass destruction (WMDs); and monitor any area on the globe sufficiently enough that meaningful changes can be detected and correctly interpreted in near-real-time. The persistent ISR capability would provide combatant commanders with assured and continued observational access to the multitude of elusive adversaries operating in their area of responsibility. However, is the realization of persistence currently achievable in the Department of Defense (DoD)? Insufficient intelligence collection platforms coupled with convoluted command and control responsibilities currently limit the Department's capability to achieve persistence in the near term.

ACCESSION NUMBER: ADA471464

http://handle.dtic.mil/100.2/ADA471464

Horne, Jeffrey C. ***Information Superiority as an American Center of Gravity: Concepts for Change in the 21st Century.*** Carlisle Barracks, PA: Army War College, 2000. 34p.

Abstract: America has made a choice; more than any other nation, the United States is dependent on cyberspace. We have embraced new information technologies, and the trappings of the revolution they have ignited, with unbridled enthusiasm. Our homes, schools, businesses, markets, communication systems, and transportation grids rely on information and telecommunication systems beyond expectations of only a decade ago. Accordingly, the information distribution and processing infrastructures supporting the U.S. elements of national power have become strategic assets worthy of a detailed protection plan to ensure their viability against any intruder. The U.S. Military's vision for the conduct of future wars, Joint Vision 2010, embraces these views and calls for information superiority as a baseline requirement in achieving battlefield dominance in future wars. This paper focuses on the effects of the information revolution and geostrategic change as they relate to evolving national security paradigms and developing military doctrine. We review the informational threat, examine specific incursions, and develop emotive concepts for the defense of military information networks while also presenting rationale for sharing offensive information operation capabilities with our foes. The discussion concludes with strategic recommendations to continue refinement of our efforts to achieve information superiority well into the millennium.

ACCESSION NUMBER: ADA377575

http://handle.dtic.mil/100.2/ADA377575

Jordan, Terry L. and Russell S. Voce. ***Centeralizing to Achieve Information Superiority.*** Monterey, CA: Naval Postgraduate School, 2002. 98p.

Abstract: The purpose of this thesis is to propose a potential organizational structure for effectively utilizing Information Operations (IO) within the Department of Defense (DOD), This thesis is in response to a request for research from the vice commander of the 193 Special Operations Wing. According to this individual, the FY 1999 Joint Warfighting Capabilities Assessment, IO panel cycle, highlighted various

deficiencies ranging from inadequate manning and force structure, to ineffective planning and integration processes, to inadequate capabilities available to support CINC requirements. Currently no one federal agency or military department has total responsibility or authority to bring all the disparate, but dependent, IO function/requirements together. As a result, funding, personnel resourcing, and control is fragmented to the detriment of the nation's warfighting capabilities. As demonstrated by the above finding, the subject of IO has pervaded numerous warfighting commands, doctrinal documents, and future vision plans. Despite this pervasion, there is no single agency within DOD that has the sole responsibility for providing or prosecuting information operations. The thesis will answer the question: What is an effective organizational structure for providing information operations that produces the synergistic effects of centralization without reducing the gains achieved at unit levels by having a decentralized approach? The answer to this question will provide an organizational model that may be applied to any individual service, or DOD as a whole, to provide an organized approach to IO. The authors of this thesis do not contend that this model will be the only way to organize for IO, only one way to organize for IO.

ACCESSION NUMBER: ADA404868

http://handle.dtic.mil/100.2/ADA404868

http://bosun.nps.edu/uhtbin/hyperion-image.exe/02Jun%5FJordan%5FVoce.pdf

Kardos, Thomas J. ***Information Superiority: Seeking Command of the Cyber-Sea.*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2000. 63p.

Abstract: *This thesis examines the initial effort to formulate principles for information-based operations. Although it is impossible to explore each aspect of this transformation, it is worthwhile to examine current efforts by the US military to develop a doctrinal foundation for Information Operations (10). It explores the ongoing struggle to capture within the confines of Joint military doctrine those critical features of this "new age driven by information". The world community is increasingly dependent on reliable information traffic. Information has become a commodity and source of power unto itself. Alvin Toffler describes this period as the transformation of societies from second-wave (industrial/mechanical) to third-wave' (information-based) means. The growing dependence of the US military on these infrastructures reveals potentially vulnerable elements of the National Information Infrastructure (NII). This monograph examines the need for a comprehensive 10 doctrine. It yields a critical analysis of existing doctrine, illuminates several flaws within the current construct, and concludes with a suggested model for 10 development. Doctrinal models are developed for the Army, Air Force, and Navy respectively. These models explain those aspects which most essentially describe the doctrinal culture' of each service component. These factors include: service organization; employment of forces (both in peace and during crisis); and methods of control. In turn, each component model is compared to the revised 10 model.*

ACCESSION NUMBER: ADA381827

http://handle.dtic.mil/100.2/ADA381827

Kaye, Tom and George Galdorisi. ***Achieving Information Superiority in Coalition Operations: Seven Imperatives for Success.*** San Diego, CA: Space and Naval Warfare Systems Center, 2002. 22p.

Abstract: *The importance of C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) as a key enabler for warfighting success has long been recognized. What has been less clear is a means for coalition forces to achieve information superiority and C4ISR dominance. Understanding not just the operational needs and the technical requirements but also the functional capabilities required to achieve this goal can hasten the day when C4ISR dominance for coalition forces is more than a futuristic goal. We address a critical issue-how does the technical community achieve this goal? The overarching thesis of this paper is that in order to achieve information superiority and C4ISR dominance, the technical community should neither chase means to overcome extant enemy operational capabilities nor attempt to push systems to the operational forces based solely on available technology. Rather, it should build to a discrete set of functional capabilities to achieve information superiority. This paper identifies seven functional imperatives to achieve this C4ISR dominance over an adversary. We conclude that what has remained timeless from the days of Sun Tzu to*

today's conflicts are the universal needs of warfighters to have the right information, at the right place, at the right time.

ACCESSION NUMBER: ADA467611

http://handle.dtic.mil/100.2/ADA467611

Kren, James. ***Collaborative Exploitation and Analysis: Helping the Joint Force Commander Achieve Information Superiority***. Newport, RI: Naval War College, February 1998. 28p.

Abstract: The National Imagery and Mapping Agency's (NIMA) new concept of Collaborative Exploitation and Analysis provides a virtual staff that can augment the Joint Force Commander (JFC) during mission analysis, planning, and execution. By 2010, Collaborative Exploitation and Analysis will help the JFC achieve information superiority provided the JFC understands what it can do for him and therefore knows to ask for this help. Collaborative Exploitation and Analysis is the advancement of these technological capabilities to achieve a network of imagery and geospatial databases, and dynamic workgroups to resolve time critical issues. Information superiority is significant to the JFC because constant knowledge about the battlespace improves mission effectiveness. Information superiority supports operational art concepts. Requirements for achieving information superiority are battlespace awareness, effective employment of forces, and a communications grid (network) that ensures uninterrupted uncorrupted service. Since October 1996, NIMA has been striving to move the imagery and geospatial communities closer together through its leadership of the United States Imagery and Geospatial Information System (USIGS). In this role, the agency is developing an end to end architecture to provide an environment that ensures the information edge.

ACCESSION NUMBER: ADA348445

http://handle.dtic.mil/100.2/ADA348445

Kuperman, Gilbert G., Randall D. Whitaker and Scott M. Brown. ***Cyber Warrior: Information Superiority Through Advanced Multi-Sensory Command and Control Technologies.*** Brooks AFB, TX: Air Force Research Laboratory, Human Effectiveness Directorate, 2000. 10p.

Abstract: This paper explores the functions of a conceptual, future watch center whose mission is to support Air Force information assurance requirements. A cognitive systems engineering approach is described through the insertion of multi-sensory, user interface technologies may be accomplished.

ACCESSION NUMBER: ADA430189

http://handle.dtic.mil/100.2/ADA430189

Lasley, Jennifer. ***Denial and Deception: A Serious Threat to Information Superiority?*** Washington, DC: National War College, 2000. 15p.

Abstract: Today's military vision of the future, embodied in the Chairman's Joint Vision documents, paints an impressive picture of the future battlespace where US forces are superior in every dimension largely because of two critical enabling factors: technology innovation and information superiority. Information superiority, in fact, underpins each of the four new concepts of future warfare: dominant maneuver, precision engagement, focused logistics and full-dimensional protection. Achieving information superiority, however, will be difficult, if not impossible, due to a host of issues, the most pernicious of which is the enemy's ability to conduct successful denial and deception (D&D) operations. Foreign actors increasingly are using D&D as an important part of an asymmetric strategy to counter overwhelming US military superiority, and many of the reasons for their success are the result of US vulnerabilities. These include: ignorance of the foreign D&D threat, security negligence that provides foreign actors with a wealth of information vital to their D&D efforts, intentional release of information to foreign governments that compromises US collection assets, and American hubris that discounts the viability of such a threat. The results of these vulnerabilities can range from costly military campaigns to, to future surprise, to outright defeat in a worst case scenario. The Departments of Defense and State, together with the

intelligence community, need to address these shortfalls in order to limit future opportunities for foreign D&D exploitation and to ensure information superiority in a JV2010 or 2020 environment.
ACCESSION NUMBER: ADA431704
http://handle.dtic.mil/100.2/ADA431704

Laudy, Claire, Juliette Mattioli and Nicholas Museux. ***Cognitive Situation Awareness for Information Superiority.*** Orsay, France: Thales Research and Technology, 2006. 28p.
Abstract: We present a summary of the drawbacks and deficiencies that we noticed in the currently available Command Support Systems (CSS) and the methodology we propose to improve them: Situation Awareness support through Cognitive Fusion of Information stemmed out of document analysis. Our approach is divided into two parts: a methodology for situation representation out of document analysis and a methodology for situation analysis and reasoning to support decision-making. The situation representation part is based on the use of conceptual graphs and fusion of nodes in graph structures, whereas the situation analysis part follows Complex Event Processing methodology.
ACCESSION NUMBER: ADA474206
http://handle.dtic.mil/100.2/ADA474206

Malloy, Rodney E. ***The Fleeting Nature of Information Superiority***. Newport, RI: Naval War College, 2004. 20p.
Abstract: The United States of America has seen vast growth in the information element of power. This paper will contrast the profound impacts of information-based warfare and information warfare on modern U.S. war fighting. The idea of information superiority becoming a key enabler for U.S. operational success will be examined. War fighting concepts will be discussed in the context of information superiority, leading to the identification of critical vulnerabilities. Finally, a strategy will be outlined to quantify these vulnerabilities and lead to development of operational war fighting concepts to achieve information superiority verses an information age adversary.
ACCESSION NUMBER: ADA425930
http://handle.dtic.mil/100.2/ADA425930

McIntosh, Gary A. ***Information Superiority and Game Theory: The Value of Varying Levels of Information.*** Monterey, CA: Naval Postgraduate School, 2002. 103p.
Abstract: The ability to acquire and use information superiority to enhance combat power and contribute to the success of military operations is a primary factor in the fulfillment of the tenets of Joint Vision 2020. This thesis examines how various levels of information and information superiority affect strategy choices and decision-making in determining the payoff value for opposing forces in a classic zero-sum two-sided contest. The results show that if opposing forces possess options with equivalent strategic capabilities, the payoff advantage is determined by the quantity of choices from which to choose. The degree of advantage in payoff for the force wide superior information is determined by the amount of choices and the quantify of bad information for the opponent. When a force possesses significantly fewer strategic options, more superior information is required to assume a payoff advantage, and for a force having more flexibility, significantly less information is required to affect an advantage in payoff. Additionally, we see that the effects of intelligence provides the greatest payoff advantage when a force possesses its maximum number of strategic options combined with the opposition also having its maximum number of choices.
ACCESSION NUMBER: ADA402744
http://handle.dtic.mil/100.2/ADA402744
http://bosun.nps.edu/uhtbin/hyperion-image.exe/02Mar_McIntosh.pdf

Miller, Russell F. ***Developing and Retaining Information Warriors: An Imperative to Achieve Information Superiority.*** Carlisle Barracks, PA: Army War College, 2000. 38p.

Abstract: Developing effective policy, doctrine, organizations, technology, and most importantly, skilled people are essential to ensure our warfighters enjoy information superiority across the spectrum of conflict. In this context, "information warriors"-people skilled in the art of conducting information operations-are essential to achieving information superiority. Information warriors must be multi-skilled-at a minimum, proficient in operations, intelligence and information technologies. Unfortunately, all military services face significant challenges in retaining information technology (IT) professionals-people with many of the critical skills needed to conduct effective information operations. This paper analyzes Air Force IT retention and its impact on achieving information superiority. In this context, information superiority is the desirable end-state, information operations the way to win it, and standing up a new Air Force Information Operations (IO) career field the best way to retain the IT professionals needed to achieve it. Key reasons IT professionals leave the Air Force are identified, leading to the conclusion that to improve IT retention, the Air Force must do a better job addressing both tangible and non-tangible satisfiers. Besides aiding IT retention, a separate Air Force IO career track is the best way to develop %information warriors"-the people warfighters will task to win information superiority on future battlefields. Joint vision 2010 makes it clear that attracting and retaining people with the intellect, training and motivation to prevail across the spectrum of military operations is critical to the future success of our forces. To that end, developing and retaining "information warriors" capable of conducting decisive information operations is a strategic, operational and tactical imperative. To fail in this endeavor will significantly jeopardize our ability to prevail in future conflicts.

ACCESSION NUMBER: ADA377713

http://handle.dtic.mil/100.2/ADA377713

Norton, Timothy P. ***Information Management: Is the U.S. Army prepared for Information Superiority?*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2003. 52p.

Abstract: Although the Army Vision 2010 states that one of the keys to success on the modern battlefield is to achieve information superiority, the current U.S. Army doctrine in this area does not support it. Specifically, the topic of information management, one of the fundamentals in information superiority, is lacking in the clarity and depth required to meet this lofty goal. Operational advantages of information superiority are obtained through the systematic provision of clear, accurate, and useable information. Under the current doctrine, the discussion is limited to the products and ignores the process. If a product focus is not addressed the U.S. Army will not reach the stated goal of information superiority. To understand this serious deficiency, this study examines current doctrinal definitions and concepts of information management and compared them with business and academic writings on the subject. The intent was to assess if the Army s concepts are sufficient to manage the information that we strive to create. The researched revealed that the Army is not prepared. Doctrine does not provide guidance on the concept of information management as a system. The doctrinal definitions identify products and qualities of information but fail to discuss frameworks and principles that are essential to information management. This gap in information management doctrine makes it nearly impossible to achieve the goal of information superiority. The Army must address these weaknesses in current doctrine. To improve information management, the Army must redefine the term information management in a manner that supports a systems approach, produce a conceptual framework for its application, publish principles of information management, and produce a single source document for information management doctrine.

ACCESSION NUMBER: ADA416242

http://handle.dtic.mil/100.2/ADA416242

Pease, Michael R. ***Information Superiority: 'Where's the Beef?''*** Newport, RI: Naval War College, February 1998. 23p.

Abstract: Joint Vision 2010 rests on the assumption that U.S. forces will enjoy dominant battle space knowledge or information superiority over any potential adversary by 2010. While Joint Vision 2010 points to the many positive trends in information technology and friendly C4, this is only half of the information superiority problem. Information superiority also includes Intelligence, Surveillance and Reconnaissance (ISR) The nature of C4 information fundamentally different from that of ISR. While information age advances tend to favor improved C4, they can seriously hinder ISR. In most areas and levels of imagery, signals and human ISR, the current state and trends do not guarantee information superiority in 2010.

ACCESSION NUMBER: ADA348443

http://handle.dtic.mil/100.2/ADA348443

Pee, Eng Yau. ***An Exploratory Analysis on the Effects of Information Superiority on Battle Outcomes.*** Monterey, CA: Naval Postgraduate School, 2002. 125p.

Abstract: Visions of future warfighting, such as Joint Vision 2020, emphasize using new technologies to obtain and exploit information advantages to achieve new levels of effectiveness in joint warfighting. Unfortunately, our warfighting models are notoriously poor at capturing the effects of information on battle outcomes. Moreover, traditional measures of effectiveness (MOEs) usually ignore the effects of information and decision making on battle outcomes. The Department of the Navy and other DoD organizations have tasked RAND to create a framework for developing measures and metrics to assess the impact of C4ISR systems and procedures on battle outcomes. In order to quantify the effects of information and decision making on battle outcomes, RAND built a deterministic model and hypothesized a scenario involving the search for, and destruction of a time-critical target (TCT). This thesis extends their work by making the simulation stochastic and exploring practical issues such as: (1) the effects of improved C4ISR systems and procedures on battle outcomes; (2) which messaging and data processing delay reductions give the greatest improvements in kill probability; (3) which command and control architecture provides the highest kill probability.

ACCESSION NUMBER: ADA402716

http://handle.dtic.mil/100.2/ADA402716

http://library.nps.navy.mil/uhtbin/hyperion/02Mar_Pee.pdf

Price, Judith M. ***Information Superiority and Geographic Information Systems: Where Is the U.S. Army?*** Fort Leavenworth, KS: Army Command and General Staff College, 2003. 46p.

Abstract: The Joint Staff published Joint Vision documents in 1996 and 2000 to provide the joint conceptual framework for the transformation effort. The United States Army embarked upon its own transformation towards its Objective Force in conjunction with the Joint Vision. Both initiatives depend upon realizing the potential of information age technologies and exploiting the information superiority to which those technologies contribute. Geospatial information provides the foundation for information superiority, which in turn supports the initiatives embodied in Army transformation and the tenets of Joint Vision. Geospatial information references locations on the surface of the earth incorporating the domains of land, sea, air and space and, as such, becomes the foundation upon which all other battlespace information is integrated. Geospatial information provides the basic framework for battlespace visualization, planning, decisions and actions. Without geospatial information, information superiority and subsequently decision superiority cannot succeed. While significant progress has occurred technologically, challenges remain with systems interoperability, training and support agencies. Part of the challenge rests in changing the experiential mindset but this is the way we have always done it in ensuring the United States Army's acquisition systems develop interoperable technological applications based on a sole common geospatial information baseline and revising the education and training systems that support the military and its support agencies. In conclusion, geospatial information is a relevant enabler but still requires continued refinements to meet the demands of Joint Vision and Army transformation in developing current and future requirements.

ACCESSION NUMBER: ADA416084
http://handle.dtic.mil/100.2/ADA416084

Van Haperen, Kees. ***Working Towards Information Superiority: Application Coherence for Digitisation Programmes - A Method for Coherently Defining Requirements for Future Command and Control Information Systems.*** Hampshire, UK: HI-Q Systems Ltd., 2003. 41p.

Abstract: Within the UK, a conceptual model has been developed which represents the main processes of the Army, i.e. the Army Activity Model (AAM). It predominantly illustrates information dependencies between processes and information elements that are exchanged between them. Over the last 18 months, the AAM has significantly matured. Moreover, there is a better understanding of its relevance for current and future Information Systems. A methodology has recently been developed that enables the richness of the AAM to be exploited for developing new C2 Information Systems (IS). By using this methodology coherent development and definition of user requirements can be achieved. In addition, the methodology enables, albeit at a high level, the assessment of coherence between C2IS and, more specifically, the processes and information that these systems support. Using UK Case Study based on the development of Joint Fire Support (JFS) Battlefield Information System Application (BISA), it is explained how the methodology allows the use of the AAM for development of new CCIS. It is explained various Soft Systems Methodology (SSM) and Modelling techniques helped to relate the JFS BISA to the AAM and define or validate coherent user requirements. Using the AAM, application coherence can be assessed and visualized at both informatics as well as technology levels. Although such assessments are conducted at a high level, they nevertheless provide detailed information on gaps and overlaps in the definition of IS requirements. This information could be used to improve requirements definition and aid coherent and interoperable system development. Finally, they will attempt to contrast the application coherence method with the COBP.

ACCESSION NUMBER: ADA
http://handle.dtic.mil/100.2/ADA425306

Zum Brunnen, Richard L., et al. **Information Operations Vulnerability/Survivability Assessment (IOVSA): Process Structure.** Aberdeen Proving Ground, MD: Army Research Laboratory, 2000. 67p.

Abstract: The Survivability/Lethality Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) has developed an information operations vulnerability/survivability assessment (IOVSA) process. The objective of the IOVSA process is to establish a systematic approach that permits analysis and evaluation of the survivability of military component level and weapon systems that include information technology (IT) items. The process will apply throughout the life cycle phases of any Department of Defense (DOD) system that collects, stores, transmits, or processes classified and/or sensitive but unclassified (SBU) information, as well as commercial components to DOD systems. The IOVSA process fulfills many of those process activities required by the DOD In formation Technology Security Certification and Accreditation Process (DITSCAP) by providing much of the required vulnerability information. The IOVSA plan for a particular system is a focused plan that has been designed to provide the decision-makers with the necessary information to make informed decisions concerning the susceptibilities and vulnerabilities of the system to information operations (10) threats. By addressing the 10 threats, the system will significantly improve its survivability by planning for both avoiding and withstanding potential problems with 10-based threats. This report discusses the IOVSA process in detail.

ACCESSION NUMBER: ADA381117
http://handle.dtic.mil/100.2/ADA381117

Cyber Warfare

Books

Alexander, Yonah and Donald J. Musch (eds.) **Cyber Terrorism and Information Warfare.** Dobbs Ferry, NY: Oceana Publications, 1999. 4 vols.
DKL U163 .C9333 1999 v. 1-4 GENERAL

Amoroso, Edward G. **Cyber Security.** Summit, NJ: Silicon Press, 2007. 177p.
Contents: An introduction to cyber security -- Understanding cyber attack -- Effects of cyber attack -- Government issues in cyber security -- Cyber security vulnerabilities -- Cyber security
DKL U 163 .A525 2007 GENERAL

Anderson, Robert H. and Anthony C. Hearn. **An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After . . . in Cyberspace II."** Santa Monica, CA: Rand, 1996. 67p.
http://www.rand.org/pubs/monograph_reports/2007/MR797.pdf
DKL TK5105.59 .A52 1996 GENERAL

Arquilla, John and David F. Ronfeldt. **Cyberwar is Coming!** P-7791. Santa Monica, CA: Rand, 1992. 35p.
http://www.rand.org/pubs/reprints/2007/RAND_RP223.pdf
DKL U163 .A76 1992 GENERAL

_____. "Cyberwar is Coming!" p. 24-50, IN: Stocker, Gerfried and Christine Schopf (eds). **Infowar**. Ars Electronica Symposium (1998: Linz, Austria). New York: Springer-Verlag Wien, 1998. 302p.
DKL U163 .I546 1998 GENERAL

Bunker, Robert J. **Five-Dimensional (Cyber) Warfighting: Can the Army After Next Be Defeated By Technologies?** Carlisle Barracks, PA: Army War College, Strategic Studies Institute, 1998. 42p.
http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=233

Campen, Alan D. and Dearth, Douglas H., eds. **Cyberwar 2.0: Myths, Mysteries and Reality**. Fairfax, VA: AFCEA International Press, 1998. 403p.
DKL UA23 .C93 1998 GENERAL

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden (eds.). **Cyberwar: Security, Strategy, and Conflict in the Information Age**. Fairfax, VA: AFCEA International Press, 1996. 296p.
DKL U163 .C94 1996 GENERAL

Center for Strategic and International Studies (Washington, D.C.) **Cybercrime ... Cyberterrorism ... Cyberwarfare: Averting an Electronic Waterloo**. Washington, DC: The Center for Strategic International Studies Press, 1998. 73p.
DKL U163 .C92 1998 GENERAL

Guisnel, Jean. **Cyberwars: Espionage on the Internet**. New York: Plenum Trade, 1997. 295p.
DKL HV6773 .G8513 1997 GENERAL

Gumahad, Arsenio T., II. **Cyber Troops and Net War: The Profession of Arms in the Information Age**. Maxwell AFB, AL: Air University, Air War College, April 1996. 57p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1506

Hoffman, Bruce. **Responding to Terrorism Across the Technological Spectrum**. Carlisle Barracks, PA: Army War College, Strategic Studies Institute, 1994. 32p.
http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=277

Hundley, Richard O. **Security in Cyberspace: Challenges for Society: Proceedings of an International Conference**. Santa Monica, CA: Rand Corporation, 1996. 59p.
http://www.rand.org/pubs/conf_proceedings/2007/CF128.pdf
DKL TK5105.59 .S4 1996 GENERAL

Lewis, James A. **Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.** Washington, DC: Center for Strategic & International Studies, 2002. 12p.
http://www.shaneland.co.uk/ewar/docs/dissertationsources/institutionalsource1.pdf

Rattray, Gregory J. **Strategic Warfare in Cyberspace**. Cambridge, MA: MIT Press, 2001. 517p.
DKL U163 .R29 2001 GENERAL

Robins, J. P. “Military Adventures in Cyberspace.” p. 2-42, IN: **Proceedings of the Second International Symposium on Command and Control Research and Technology.** Market Bosworth, United Kingdom, 24-26 June 1996. Washington, DC: National Defense University, 1997. 592p.
DKL UB212 .I573 1996 GENERAL

Ware, Willis H. **The Cyber-Posture of the National Information Infrastructure**. Santa Monica, CA: Rand, 1998. 37p.
http://www.rand.org/pubs/monograph_reports/2007/MR976.pdf
DKL TK5102.85 .W37 1998 GENERAL

Periodicals

Alford, Lionel D., Jr. “Cyber Warfare: Protecting Military Systems.” **Acquisition Review Quarterly**, Spring 2000, v. 7, no. 2, p. 99-120.
http://www.dau.mil/pubs/arq/2000arq/alford.pdf

Allison, Gary D. “ The Cyberwar of 1997: Timidity and Sophistry at the First Amendment Front.” **Tulsa Law Journal**, Fall 1997, v. 33, no.1, p. 103-134.

Andrews, Robert E.. “Cyber Terrorism, a Real Threat to Society.” **Congressional Record**, March 14, 2000, v. 146, no. 28, p. H974-H979.

Armstrong, Helen L. and Jack Davey. “Teaching Competitive Intelligence and Cyberwarfare in a Business Context.” **Journal of Information Warfare**, 2003, v. 2, no. 3, p. 1-7.

Arquilla, John. “The Great Cyberwar of 2002.” **Wired**, February 1993, v. 6, no.2, p. 122+
http://www.wired.com/wired/archive/6.02/cyberwar.html

Arquilla, John and David Ronfeldt, "Cyberwar is Coming!" **Comparative Strategy**, April–June 1993, v. 12, no. 2, p. 141-166.

Bunker, Robert J. “Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXI.” **Parameters**, Autumn 1996, v. 26, no. 3, p. 108-120.

Clemmons, Buard Q. and Gary D. Brown. “Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction.” **Military Review**, September/October 1999, v. 79, no. 5, p. 35-45.

Coale, John C. ”Fighting Cybercrime.” **Military Review**, March-April 1998, v. 78, no. 2, p. 77-82.

Cooper, Pat. “Cyberwar Recasts National Security.” **Army Times**, June 26, 1995, v. 55, no. 48, p. 26.

Correll, John T. "War in Cyberspace." **Air Force Magazine**, January 1998, v. 81, no. 1, p. 32-36.

Covault, Craig. "Cyber Threat Challenges Intelligence Capability NSA Director Warns of `Fundamental New Danger,' Cites Changing Role of Defensive Systems and Intelligence." **Aviation Week & Space Technology**, February 10, 1997, v. 146, no. 6, p. 20+

Cross, Michael. “Threat of Cyber Sabotage Increases.” **Computers & Security**, 1999, v. 18, no. 5, p. 434-435.

“Cyber War Threat Is Real and Growing.” **Aviation Week & Space Technology**, April 27, 1998, v. 148, no. 17, p. 78+

"Cyberterrorism Hype." **Jane's Intelligence Review**, December 1999, v. 11, no. 12, p. 48-52.

Davey, Jack and Helen L. Armstrong. “An Approach to Teaching Cyber Warfare Tools and Techniques.” **Journal of Information Warfare**, December 2001, v. 1, no. 2.

_____. “Dominating the Attacker: Use of Intelligence and Counterintelligence in Cyberwarfare.” **Journal of Information Warfare**, October 2002, v. 2, no. 1, p. 23-31.

Evers, Stacey. “Stopping the Hacking of Cyber Information.” **Jane’s Defence Weekly**, April 10, 1996, v. 25, no. 15, p. 22-25.

Forster, Anthony. “Hi-Tech Terrorists Turn to Cyber Warfare.” **Jane's Intelligence Review**, September 1999, v. 11, no. 9, p. 46-49.

Fulghum, David A. “Cyberwar Plans Trigger Intelligence Controversy: U.S. National Intelligence Agencies, Military at Odds Over What Can be Attacked in a Computer War.” **Aviation Week & Space Technology**, January 19, 1998, v. 148, no. 3, p. 52-54.

Gengler, Barbara. “Cyberattacks...US goes on the Offensive.” **Computer Fraud & Security**, 2000, v. 2000, no. 2, p. 5.

_____. “Cyberwarfare From a Concerned Citizen!” **Computer Fraud & Security**, January 2000, v. 2000, no. 1, p. 5-6.

Gray, Colin S. “Three Visions of Future War.” **Queen's Quarterly**, Spring 1996, v. 103, no. 1, p. 35-49.

Hancock, Bill. “And If That is Not Enough – Mainland China and Taiwan Engage in Cyberwar.” **Computers & Security**, 1999, v. 18, no. 6, p. 465-466.

Hinde, Stephen. “Cyber Wars and Other Threats.” **Computers & Security**, 1998, v. 17, no. 2, p. 115-118.

Hum, Peter. “Preparing for Cyberwar.” **Computers & Security**, 1997, v. 16, no. 2, p. 127.

Hundley, R. and R. Anderson. "Emerging Challenge: Security and Safety in Cyberspace." **IEEE Technology and Society Magazine**, Winter 1995-1996, v. 14, no. 4, p. 19-28.

Kaneshige, Thomas. “CIA Plans Cyberwar Defence Centre.” **Computer Fraud & Security**, 1996, v. 1996, no. 8, p. 8.

_____. “Is the US Prepared for Cyberwar?” **Computer**, July 1996, v. 29, no. 7, p. 20-21.

Knapp, Kenneth J. and William R. Boulton. “Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments.” **Information Systems Management**, Spring 2006, v. 23, no. 2, p. 76-87.

Luzwick, Perry. “Crackers and Phreakers Conduct Better Coherent Knowledge-Based Operations Than Most Companies.” Part 3 of 4. **Computer Fraud & Security**, 2000, v. 2000, no. 3, p. 16-17.

Magnuson, Stew. “Cyber War.” **National Defense**, February 2006, v. 90, no. 627, p. 30-31.

Mann, Paul. "Cyber Threat Expands With Unchecked Speed." **Aviation Week & Space Technology**, July 8, 1996, v. 145, no. 2, p. 63-64.

_____. “Government/Industry Alliance Urged Against Cyber Threats.” **Aviation Week & Space Technology**, July 13, 1998, v. 149, no. 2, p. 65-67.

Matthews, William. “Girding for Cyberwar.” **Air Force Times**, July 18, 1994, v. 54, no. 50, p. 36; **Army Times**, July 18, 1994, v. 54, no. 51, p. 36; **Navy Times**, July 18, 1994, v. 43, no. 41, p. 36.

Matthews, William. “Pentagon Task Forces Will Assist Civilian Authorities.” **Air Force Times**, October 25, 1999, v. 60, no. 12, p. 18.

Mehdizadeh, Yahya. “Transit, Infrastructure Still Top Worry, but Cyber War Looms.” **Security**. September 2007, v. 44, no. 9, p. 136+

“No Sheriffs Patrol Universal Cyberspace Frontier Towns.” **Signal**, June 1996, v. 50, no. 10, p. 39-42.

Penenberg, Adam L. “A Private Little Cyber war.” **Forbes**, February 21, 2000, v. 165, no. 4, p. 68-70.

Pollitt, Mark M. “Cyberterrorism - Fact or Fancy?” **Computer Fraud & Security**, 1998, v. 1998, no. 2, p. 8-10.

Pringle, Caleb A. “Terrorist Organizations' Use of Information Age Capabilities.” **Defense & Foreign Affairs Strategic Policy**, 1999, v. 27, no. 1, p. 9-12.

Radcliff, Deborah. “Hackers, Terrorists, and Spies.” **Software Magazine**, October 1997, v. 17, no. 11, p. 36-47.

Ramos, B. J. “Standing Cyberwatch.” **Navy Times**, July 6, 1998, v. 47, no. 39, p. 19.

Rathmell, Andrew. "Cyber-Terrorism: The Shape of Future Conflict?" **RUSI Journal**, October 1997, v. 142, no. 5, p. 40-45.

Sakkas, Peter E. “Espionage and Sabotage in the Computer World.” **International Journal of Intelligence and Counterintelligence**, Summer 1991, v. 5, no. 2, p. 155-202.

Sandberg, Jared. “Holes in the Net.” **Newsweek**, February 21, 2000, v. 135, no. 8, p. 46-49.

Sawyer, Tom. “Protecting Electronic Data Becomes a Burning Issue: Cyber Assaults and Terrorism Put Security on the Front Burner.” **ENR**, November 5, 2001, v. 247, no. 19, p. 19-24.

Schneider, James J. "A New Form of Warfare." [Cybershock]. **Military Review**, January-February 2000, v. 90, no. 1, p. 56-61.

“Science and Technology: Cyber Wars.” **The Economist**, January 13, 1996, v. 338, no. 7948, p. 77+

Seffers, George I. “U.S. Could be the Loser in a Worldwide Cyber War.” **Federal Times**, August 9, 1999, v. 35, no. 27, p. 7+

Shimeall, Timothy, Phil Williams and Case Dunlevy. “Countering Cyber War.” **NATO Review**, Winter 2001/2002, v. 49, no. 16-18.

Skaggs, Michael D. “Digital Command and Control: Cyber Leash or Maneuver Warfare Facilitator?” **Marine Corps Gazette**, June 2003, v. 87, no. 6, p. 46-48.

Snell, Albert E. and Edward J. Keusenkothen. "Mass Destruction Weapons Enter Arsenal of Terrorists." **National Defense**, January 1995, v. 79, no. 504, p. 20-21.

Soo Hoo, Kevin, Seymour Goodman and Lawrence Greenberg. "Information Technology and the Terrorist Threat." **Survival**, Autumn 1997, v. 39, no. 3, p.135-155.

Stanton, John J. “Rules of Cyber War Baffle U.S. Government Agencies.” **National Defense**, February 2000, v. 84, no. 555, p. 29-30.

Stauffer, Don. “Electronic Warfare: Battles Without Bloodshed.” **Futurist**, January/February 2000, v. 34, no. 1, p. 23-26.

Strobel, Warren P. “A Glimpse of Cyberwarfare.” **U.S. News & World Report**, March 13, 2000, v. 128, no. 10, p. 32-33.

Tenet, George J. “Cyber War is Real and Growing.” [Excerpts from Address]. **Aviation Week & Space Technology**, April 27, 1999, v. 148, no. 17. p. 78.

Vistica, Gregory. “Cyberwar and Sabotage.” **Newsweek**, May 31, 1999, v. 133, no. 22, p. 38.

_____. “’We’re in the Middle of a Cyberwar.’” **Newsweek**, September 20, 1999, v. 134, no. 12, p. 52.

Waller, Douglas C. “Onward Cyber Soldiers.” **Time**, August 21, 1995, v. 146, no. 8, p. 38-44.

Walsh, Mark. “Cyberspace: the Services' Next Battleground.” **Army Times**, June 2, 1997, p. 23.

Wang, Huasqing and Shuozhong Wang. “Cyber Warfare: Steganography vs. Steganalysis.” **Communications of the ACM**, October 2004, v. 47, no. 10, p. 76-82.

Whine, Michael. “Cyberspace – A New Medium for Communication, Command, and Control by Extremists.” **Studies in Conflict & Terrorism**, July-September 1999, v. 22, no. 3, p. 231-246.

Williams, Robert H. “Intelligence Community Girds for Cyberwar; Major Snafus Possible with Low Tech Efforts.” **National Defense**, October 1998, v. 83, no. 541, p. 4.

Witt, Mike. “Computers, Communications and Cyberwar.” **Asian Defence Journal**, February 1998, p. 58.

Documents, Theses & Technical Reports

Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography.

Are, David C. ***When Does a "Hacker" Become an "Attacker?"*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, December 1998. 61p.

Abstract: The ability to defend the United States cyber sovereign territory is a must for the country to continue to enjoy relative freedom. The actual defense of this is far more difficult than the traditional defense of land, sea or air space. The Internet offers an environment of exponential growth in both technology and users. Couple this with an infantile and developing governing system and the Internet is both a conduit for use and a vehicle for attack. The history of cyber attack is key in determining the ability to defend and the mode in which to do it. By tracing the capabilities of adversaries, both internal and external, we can attempt to delineate the point where the electronic intrusion becomes alarming to the nation. Combine this understanding with a thorough knowledge of current methodologies and tools used for cyber attack and one has a good jump on "knowing one's enemy." Constraining, yet legitimizing, the effort of governments to fight the unbounded attack of cyber warriors are laws and agreements which attempt to lay ground rules for cyber utilization. Careful construction of these rules joined with vigilant international agreements can facilitate apprehension and thwarting of would-be attackers worldwide. Laws which are drafted without thought to the defense of information systems can be equally as damaging to the government that adopts them. This monograph concludes with the current efforts underway by the United States government and the Department of Defense in particular. Presidential Decision Directives 62 and 63 posture the United States for success in combating cyber aggression. The follow through by the legislative, judiciary branches and various departments will determine the success of this country in securing its national information infrastructure.

ACCESSION NUMBER: ADA366206

http://handle.dtic.mil/100.2/ADA366206

Duklis, Peter S., Jr. ***The Joint Reserve Component Virtual Information Operations Organization (JRVIO); Cyber Warriors Just a Click Away.*** Carlisle Barracks, PA: Army War College, 2002. 32p.

Abstract: Informational power has now been coined as a national power along with political, economic and military powers. Moreover, Information Operations (IO) is a key stratagem to protect and facilitate our national interests across the full spectrum of engagement. The Department of Defense (DoD) incorporates information operations as part of all of its current plans, operations and exercises. Yet, there are very few organizations dedicated solely to IO. However, DoD conducted the Reserve Component Employment 2000-2005 (RCE-05) Study in which it was directed that a Joint Reserve Component Virtual Information Operations Organization (JRVIO) be established to support joint and inter-agency organizations. In this paper, I will determine what virtual means, how it will be used for IO, and how a joint reserve unit is structured and functions. Furthermore, I will make a recommendation on how and where this/these JRVIO(s) should be utilized to support overall DoD Information Operations and specifically, Joint Commands and inter-agency organizations.

ACCESSION NUMBER: ADA404656

http://handle.dtic.mil/100.2/ADA404656

Glass, Deborah P. ***Cyberterrorism Versus Cyberwar: at What Point Does Department of Justice Turn Over Cyber Incidents to the Department of Defense?*** Carlisle Barracks, PA: Army War College, 2001. 28p.

Abstract: The United States is increasingly dependent upon technology to the extent that every facet of the Nation's critical infrastructure (CI) depends on computer technology at some level. The conduct of future warfare, both offensively and defensively, is also increasingly technological. The realization that the U.S. is extremely vulnerable to asymmetric warfare via the Internet and to acts of terrorism was part of the driving force behind the development of PDD 63. Because of the widespread dependence on the CI, consideration is being given to assigning ultimate responsibility over these interconnected systems to a single agency. Currently the Federal Bureau of Investigation (FBI) has cognizance over items relating to terrorism. The Department of Defense has responsibility when it comes to acts of war. The line between terrorism and warfare over the Internet is ambiguous, as are the lines of authority. This paper will examine the definitions of terrorism and warfare where the Global Information Infrastructure and other components of our nation's CI are concerned. At what point, and by what mechanism should responsibility and authority be transferred from the FBI to the DoD? Should a different, perhaps even a new, agency be given ultimate response responsibility for attacks on the CI?

ACCESSION NUMBER: ADA390624

http://handle.dtic.mil/100.2/ADA390624

Haber, Matthew E. ***Computer Network Attack and the Laws of Armed Conflict: Searching for Moral Beacons in Twenty-First-Century Cyberwarfare.*** Fort Leavenworth, KS: Army Command and Staff College, 2002. 123p.

Abstract: Computer network attack ushered in change for the profession of arms. Militaries achieve effects using computers, previously attained only through physical destruction. Computer network attack's problem is it operates outside the observable domain the laws of armed conflict describe, yet its effects are what the laws address. Thus, the primary research question is: Does a legal framework of analysis exist for computer network attack? The secondary question became: If a framework exists, is it applied consistently throughout the Department of Defense? A search of literature and interviews with information operators and their associated lawyers revealed a framework by Thomas Wingfield. The framework analyzes the level of force but does not address the four basic principles for warfare; military necessity, humanity, proportionality, and discrimination. Also, the framework is not applied throughout the Department of Defense. The Joint Task Force Computer Network Operations' creation is the first step in building a hierarchical structure for consistent application of law to computer network attack. Research recommends such a structure expand Wingfield's framework for computer network attack to be a viable weapon for Twenty-First-Century Warfare.

ACCESSION NUMBER: ADA406496

http://handle.dtic.mil/100.2/ADA406496

Howes, Norman R., Michael Mezzino and John Sarkesian. ***On Cyber Warfare Command and Control Systems.*** Washington, DC: Missile Agency, 2004. 44p.

Abstract: As Defense agencies and services expand their reliance on computer networks, risk to information availability and integrity increases. It is no longer adequate to rely solely on the now traditional defense-in-depth strategy. We must recognize that we are engaged in a form of warfare, cyber warfare, and deploy our resources using the strategy and tactics of warfare. Most Defense organizations have not yet developed strategies or tactics for cyber warfare. This causes security devices to be used ineffectively and responses to be untimely. Cyber warfare then becomes a one-sided battle where the attacker makes all the strikes and the target of the attack responds so slowly that the attacker usually gets away without being identified. Employing cyber warfare strategy and tactics requires a cyber warfare command and control system. Responses to cyber attacks do not require offensive measures outside our own network boundaries to be effective, but they do require timely responses. Timely offensive action taken within our own network boundaries can lead to an identification of the attacker. During the past two years we have

developed a prototype cyber warfare command and control system to demonstrate that defense-in-depth can be taken to a new level that is active and anticipatory rather than passive and reactive.
ACCESSION NUMBER: ADA465692
http://handle.dtic.mil/100.2/ADA465692

Knapp, Kenneth J. ***Cyber Warfare: Raising Information Security to a Top Priority***. Wright Patterson AFB, OH: Air Force Institute of Technology, 2004. 34p.
Abstract: Beyond the media hype, information warfare has become a central concern of the Internet age. While not denying the obvious military implications, a 15-year review (1990-2004) of information conflict reveals twelve characteristics and trends that affect civilian communities as well. For example, there is the growing availability of low-cost cyber weaponry on the Internet as modern societies increasingly rely on information infrastructures, and civilian organizations become the primary targets of attacks. Additionally, information warfare encompasses such domains as espionage, media perception, nation-state relations, and transnational criminal activities. As information conflict becomes a growing concern, managers must understand this reality and plan to defend against attacks. As a conclusion, this article provides a summary of the twelve selected characteristics of information conflict and offers a comprehensive strategy to promote effective information security in organizations.
ACCESSION NUMBER: ADA425352
http://handle.dtic.mil/100.2/ADA425352

Mays, John B. ***Cyberwar as Anti-War: The Keystroke is Mightier than the Sword.*** McLean, VA: Booz-Allen and Hamilton, 1998. 8p.
Abstract: This report relates examples of wars in the past as wars to that utilize the power of information. Cyberwar is another powerful type of war that can be described as "actions taken during times of crisis or conflict (including war) to affect adversary information and information systems while defending one's own information and information systems." Computer network attack is a derivative of the commercial sector.
ACCESSION NUMBER: ADA399582
http://handle.dtic.mil/100.2/ADA399582

O'Hara, Timothy F. ***Cyber Warfare/Cyber Terrorism*****.** Carlisle Barracks, PA: Army War College, 2004. 35p.
Abstract: Section 1 of this paper provides an overview of cyber warfare as an element of information warfare, starting with the general background of the current strategic environment the United States is operating in. This section also examines why information warfare has become such an attractive alternative form of conflict, reviews the traditional principles of warfare and why they may or may not apply to cyber warfare, and proposes new principles of warfare that may be needed to conduct cyber warfare. Section 1 concludes with a review of offensive and defensive cyber warfare concepts. Section 2 presents a general overview of cyber terrorism, including definitions of cyber terrorism and cyber terrorism support. This section examines three possible levels of cyber terrorist attack and concludes with an analysis of the factors that may or may not encourage terrorists to engage in cyber terrorist operations. The third and final section of the paper attempts to answer the following question: "Is cyber terrorism a legitimate threat?" This section examines factors that should be considered when evaluating cyber terrorism as a potential threat. (4 tables, 5 figures, 25 refs.)
ACCESSION NUMBER: ADA424310
http://handle.dtic.mil/100.2/ADA424310

Stytz, Martin R., Sheila R. Banks and Michael J. Young. ***Realistic and Affordable Cyberware Opponents for the Information Warfare Battlespace.*** Wright-Patterson AFB, OH: Air Force Research Laboratory, 2003 42p.

Abstract: As military environments increase in the complexity, fidelity, scope, and number of participants, the reliance of the military upon information superiority to facilitate successful operations increases. In conjunction with this increase upon accurate and timely information the vulnerability of military forces to information attack also increases. Additionally, information management capability improvements inevitably increase the value of the information management networks and software; thereby, directly increasing the incentive for attacking or pirating the network and software capabilities. Therefore, as the information management capabilities of military forces increase, there is a corresponding need for improved security for the software and network systems and this need for improved security will increase as the value of the software and network systems increases. This improvement in information management capabilities must be accompanied by a corresponding increase in the ability to manage the protection of military information systems, which is a topic that has received scant attention.

ACCESSION NUMBER: ADA467405

http://handle.dtic.mil/100.2/ADA467405

Tobin, Scott D. ***Establishing a Cyber Warrior Force***. Wright Patterson AFB, OH: Air Force Institute of Technology, School of Engineering and Management, 2004. 53p.

Abstract: Cyber Warfare is widely touted to be the next generation of warfare. As America's reliance on automated systems and information technology increases, so too does the potential vulnerability to cyber attack. Nation and non-nation states are developing the capability to wage cyber warfare. Historically, the Air Force and DoD have concentrated their efforts toward defensive network operations. However, a shift in doctrine has shown both the Air Force and DoD acknowledging the potential for Information Warfare. What appears to be lacking is the trained and educated cyber warrior force that will carry out the information operations if needed. This research project examines the doctrine of DoD and national agencies to engage in information operations and efforts in place to train cyber warriors. In turn, this research project offers recommendations for a career development and progression model for an Air Force Cyber Warrior force.

ACCESSION NUMBER: ADA428120

http://handle.dtic.mil/100.2/ADA428120

Network Centric Warfare

Books

Alberts, David S., et al. **Network Centric Warfare: Development and Leveraging Information Superiority**. Washington, DC: National Defense University Press, May 1999. 256p.
DKL U21.2 .A413 1998 GENERAL

_____. **Network Centric Warfare: Development and Leveraging Information Superiority**. 2nd ed. Washington, DC: National Defense University Press, September 1999. 284p.
http://www.dodccrp.org/files/Alberts_NCW.pdf

Arquilla, John and David Ronfeldt. **The Advent of Netwar**. MR-789-OSD. Santa Monica, CA: Rand, 1996. 118p.
http://www.rand.org/pubs/monograph_reports/MR789/index.html
DKL U240 .A77 1996 GENERAL

Cares, Jeffrey R. **Distributed Networked Operations: The Foundations of Network Centric Warfare.** Newport, RI: Alidade Press, 2005. 201p.
DKL UB212 .C16 2005 GENERAL

Dombrowski, Peter J., Eugene Gholz, and Andrew L. Ross. **Military Transformation and the Defense Industry After Next: The Defense Industrial Implications of Network-Centric Warfare**. Newport, RI: Naval War College, 2003. Newport Papers no. 18. 128p.
http://handle.dtic.mil/100.2/ADA421889
DKL UA18 .U5 D65 2003 GENERAL

Freedman, Lawrence. **The Revolution in Strategic Affairs**. Adelphi Papers; No. 318. Oxford: Oxford University Press, International Institute for Strategic Studies, 1998. 87p.
DKL JZ5588 .F73 1998 GENERAL

Gomez, Richard M. **Centralized Command: Decentralized Execution: Implications of Operating in a Network Centric Warfare Environment**. Maxwell AFB, AL: Air University, Air War College, 2003. 34p.
https://research.maxwell.af.mil/viewabstract.aspx?id=4743

Gumahad, Arsenio T., II. **Cyber Troops and Net War: The Profession of Arms in the Information Age**. Maxwell AFB, AL: Air University, Air War College, 1996. 60p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1506

Josephson, Edward H. **Fighting Smarter: Leveraging Information Age Technology**. Land Warfare Papers, No. 18. Arlington, VA: Institute of Land Warfare, Association of the United States Army, 1994. 21p.

Layton, P. B. **Network-Centric Warfare: A Place in Our Future?** Air Power Studies Centre paper; no. 74. Canberra, Australia: Air Power Studies Centre, Royal Australian Air Force, 1999.
DKL UB212 .L39 1999 GENERAL

Mitchell, Paul T. **Network Centric Warfare: Coalition Operations in the Age of US Military Primacy.** London: International Institute for Strategic Studies, 2006. 90p.
DKL U 21.2 .M58 2006 GENERAL

Moffat, James. **Complexity Theory and Network Centric Warfare**. Washington, DC: DoD Command and Control Research Program, 2003. 160p.
http://www.dodccrp.org/files/Moffat_Complexity.pdf
DKL U21.2 .M584 2003 GENERAL

Proceedings of the 7th International Command and Control Research and Technology Symposium. "Track 4 Network Centric Applications." Quebec, Canada, 16-20 September 2002. Washington, DC: National Defense University, 2002.
http://www.dodccrp.org/events/7th_ICCRTS/fore.htm

Proceedings of the 8th International Command and Control Research and Technology Symposium. "Track 5 Network-Centric Applications." National Defense University, Washington, DC, 17-19 September 2003. Washington, DC: National Defense University, 2003.
http://www.dodccrp.org/events/8th_ICCRTS/foreword.htm

Proceedings of the 9th International Command and Control Research and Technology Symposium. "Track 7.1 Network Centric Applications: Technology." Copenhagen, Denmark, 14-16 September 2004. Washington, DC: National Defense University, 2004.
http://www.dodccrp.org/events/9th_ICCRTS/CD/foreword.htm

Proceedings of the 2000 Command and Control Research and Technology Symposium. "Track 2 Network Centric Applications and C4ISR and Space." Naval Postgraduate School, Monterey, CA, 26 June – 28 June 2000. Washington, DC: National Defense University, 2000.
http://www.dodccrp.org/events/2000_CCRTS/index.htm

Proceedings of the 2001 Command and Control Research and Technology Symposium. "Track 5 Network Centric Applications." US Naval Academy, Annapolis, MD, 19 June – 21 June 2001. Washington, DC: National Defense University, 2001.
http://www.dodccrp.org/events/6th_ICCRTS/index.htm

Proceedings of the 2002 Command and Control Research and Technology Symposium. "Track 1 NC Applications and Space." Naval Postgraduate School, Monterey, CA, 11-13 June 2002. Washington, DC: National Defense University, 2002.
http://www.dodccrp.org/events/2002_CCRTS/fore.htm

Proceedings of the 2004 Command and Control Research and Technology Symposium. "Track 2 Network Centric Applications", San Diego, CA, 15-17 June 2004. Washington, DC: National Defense University, 2004.
http://www.dodccrp.org/events/2004_CCRTS/CD/foreword.htm

Shin, Insub and Alexander H. Levis. "Performance Prediction of a Network-Centric Warfare System." IN: **Proceedings of the 2000 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 26 June – 28 June 2000. Washington, DC: National Defense University, 2000.
http://www.dodccrp.org/events/2000_CCRTS/index.htm

Shukman, David. **The Sorcerer's Challenge: Fears and Hopes for the Weapons on the Next Millennium**. London: Hodder & Stoughton, 1995. 256p.
DKL U42 .S58 1995 GENERAL

Silbaugh, Eric E. **Network-Centric Operations – Promise, Chimera and Achilles' Heel: Challenges and Pitfalls for Networks and Information Infrastructure**. Maxwell AFB, AL: Air University, Air Command and Staff College, 2005. 39p.
https://research.maxwell.af.mil/viewabstract.aspx?id=5057

Smith, Edward R., Jr. **Effects Based Operations and Applying Network Centric Warfare to Peace, Crisis, and War**. Washington, DC: DoD Command and Control Research Program, 2002. 558p.
http://www.dodccrp.org/files/Smith_EBO.PDF
DKL UA23 .S5238 2002 GENERAL

Stein, Fred P. "Observations on the Emergence of Network Centric Warfare." p. 212-220, IN: **Proceedings of the 1998 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 29 June - 1 July 1998. Washington, DC: National Defense University, 1998. 943p.
DKL UB212 .C68 1998 GENERAL

Tuttle, Jackson. **Network Centric Warfare Fleet Battle Experiments Alpha and Bravo / Historical Documentation Conducted by Naval Reserve Combat Documentation Detachment 206**. Washington, DC: Naval Historical Center, 1998.
DKL V245 .T87 1998 GENERAL

United States. Dept. of Defense. Office of the Secretary of Defense. **Network Centric Warfare: Department of Defense Report to Congress.** CD-ROM. [Washington, DC: Dept. of Defense, 2001]
DKL QA76.9.A25 U55 2001 CIRCDESK

Vockers, Michael G. **Warfare in 2020: A Primer**. Washington, DC: Center for Strategic and Budgetary Assessments, 1996. 16p.

Wheatley, Gary F. and Fred P. Stein. “Measuring the Potential Effectiveness of Network Centric Warfare.” p. 282-294, IN: **Proceedings of the 1998 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 29 June - 1 July 1998. Washington, DC: National Defense University, 1998. 943p. **DKL UB212 .C68 1998 GENERAL**

Wheatley, Gary F. and John R. McDaniel. “Distributed Surveillance for Network Centric Warfare.” IN: **Proceedings of the 2000 Command and Control Research and Technology Symposium.** Naval Postgraduate School, Monterey, CA, 26 June – 28 June 2000. Washington, DC: National Defense University, 2000. *http://www.dodccrp.org/events/2000_CCRTS/index.htm*

Wilson, Clay. **Network Centric Warfare: Background and Oversight Issues for Congress.** RL32411. Washington, DC: Congressional Research Service, Library of Congress, 2005. *http://bosun.nps.edu/uhtbin/hyperion-image.exe/CRS-RL32411.pdf*

Periodicals

Ackerman, Robert K. “Data Holds the Key to Network-Centricity.” **Signal**, January 2005, v. 59, no. 5, p. 37-41.

_____. “Military Crystal Ball Portends Network-Centric Supremacy.” **Signal**, June 2001, v. 55, no. 10, p. 16-19.

Arquilla, John and David Ronfeldt, "The Advent of Netwar: Analytic Background." **Studies in Conflict & Terrorism**, July-September 1999, v. 22, no. 3, p. 193-206.

Ash, Lawrence N. “Fighting for Network Centric Warfare.” **United States Naval Institute Proceedings**, August 2000, v. 126, no. 8, p. 74-76.

Barnett, Thomas P.M. “The Seven Deadly Sins of Network-Centric Warfare.” **United States Naval Institute Proceedings**, January 1999, v. 125, no. 1, p. 36-39.

Blahs, Edmund C. “Network-Centric Warfare Requires a Closer Look.” **Signal**, May 2003, v. 57, no. 9, p. 56-57.

Blaker, James. “Arthur K. Cebrowski: A Retrospective.” **Naval War College Review**, Spring 2006, v. 59, no. 2, p. 129-145.
http://www.nwc.navy.mil/press/review/documents/NWCRSP06.pdf

Boorujy, James R. “Network-Centric Concepts can Guarantee Access.” **United States Naval Institute Proceedings**, May 2000, v. 126, no. 5, p. 60-63.

Bowdish, Randall G. “Network Centric Warfare: Developing and Leveraging Information Superiority.” **United States Naval Institute Proceedings**, December 1999, v. 125, no. 12, p. 78-82.

Brewin, Bob. “DOD Lays Groundwork for Network-Centric Warfare.” **Federal Computer Week**, November 10, 1997, v. 11, no. 35, p. S4-S8.

Campen, Alan D. "Joint Vision Initiates Big Challenge to Acquisition, Integration, Culture: Industry, Academia Invited to Participate in Integrated Products Team to Define Joint Network-Centric Warfare." **Signal**, October 1997, v. 52, no. 2, p. 71-73.

_____. “Look Closely At Network-Centric Warfare.” **Signal**, January 2004, v. 58, no. 5, p. 43-45.

Cebrowski, Arthur K. “President’s Notes.” **Naval War College Review**, Autumn 1998, v. 52, no. 4, p. 4-7.

_____. “President’s Notes.” **Naval War College Review**, Spring 1999, v. 53, no. 2, p. 4-11.

_____. “Sea Change [Shift From Platform-Centric to Network-Centric Warfare – Exploiting Information Superiority].” **Surface Warfare**, November-December 1997, v. 22, no. 6, p. 2-6.

Cebrowski, Arthur K. “Military Responses to the Information Age.” **RUSI Journal**, October 2000, v. 145, no. 5, p. 25-29.

_____. “Network-Centric Warfare.” **Military Technology**, May 2003, v. 27, no. 5, p.16+

Cebrowski, Arthur K. and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." **United States Naval Institute Proceedings**, January 1998, v, 124, no. 1, p. 28-35.

Cebrowski, Arthur K. and Thomas P.M. Barnett. “The American Way of War.” **United States Naval Institute Proceedings**, January 2003, v. 129, no. 1, p. 42-43.

Chen, Clement C. “Anatomy of Network-Centric Warfare.” **Signal**, August 2003, v. 57, no. 12, p. 47.

Chopra, A.C. “From Simplistic Assurances of NEC (network Enabled Capability) to Optimistic Promises of NCW (Network Centric Warfare): More Pitfalls than Promises.” **Royal Air Force Air Power Review**, Spring 2005, v. 8, no. 1, p. 52-77.

Cook, Nick. “Network-Centric Warfare--The New Face of C4I.” **Interavia**, February 2001, v. 56, no. 650, p. 37-39.

_____. “Ready for Net-Centric Warfare.” **Interavia**, March 2002, v. 57, no. 661, p. 19-21.

Cosgrove, Peter. “Racing Towards the Future: Reflections on Iraq, the Art of Command and Network-centric Warfare.” **Australian Army Journal**, December 2003, v. 1, no. 2, p. 25-33.
http://www.defence.gov.au/army/lwsc/AbstractsOnline/AAJournal/2004_S/AAJ_s_2003_03.pdf

Daembkes, Heinrich. “Network-Centric Operations and Information Superiority: Current Trends of Key Enabling Technologies.” **Microwave Journal**. (International Ed.), October 2006, v. 49, no. 10, p. 24-40.

Dahl, Erik J. “Net-Centric Before Its Time.” **Naval War College Review**, Autumn 2005, v. 58, no. 4, p. 109-135.
http://www.nwc.navy.mil/press/review/documents/NWCRAU05.pdf

Estes, Kenneth W. "Network-Centric Warfare." **United States Naval Institute Proceedings**, March 1998, v. 124, no. 3, p. 16 [letter to the editor].

Ferris, John. “Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?” **Intelligence & National Security**, Summer 2004, v. 19, no. 2, p. 199-225.

Fitzgerald, James R., et al. “Network-Centric Antisubmarine Warfare.” **United States Naval Institute Proceedings**, September 1998, v. 124, no. 9, p. 92-95.

Fowler, Michael C. “Network Centric Warfare: Developing and Leveraging Information Superiority.” **Naval War College Review**, Spring 2000, v. 53, no. 2, p. 229-231.

Friedman, Norman. “Network-Centric Warfare in the Middle East.” **United States Naval Institute Proceedings**, October 2006, v. 132, no. 10, p. 90-91.

_____. “Transformation and Network-Centric Warfare Tested in Iraq.” **United States Naval Institute Proceedings**, August 2004, v. 130, no. 8, p. 4+

Fulghum, David A. “Inside the Loop; Automated Software Tools are Crucial for Releasing the Potential of Network-Centric Warfare.” **Aviation Week & Space Technology**, December 22, 2003, v. 159, no. 25, p. 58-60.

Garstka, John J. “Network-Centric Warfare Offers Warfighting Advantage.” **Signal**, May 2003, v. 57, no. 9, p. 58-60.

Gormley, Dennis M. and Douglas M. Hart. “Extending Network-Centric Warfare to Coalition Crisis Management and Assessment.” **RUSI Journal**, April 2000, v. 145, no. 2, p. 67-72.

Green, Larry H. and Barry E. Raff. “Net-Centric Undersea Warfare.” **Sea Technology**, November 1999, v. 40, no. 11, p. 19+

Gregory, Bill. “From Stovepipes to Grids: Network-Centric Warfare Concept Spreads Among the Services; Industry's Payoff Lies in New Sensors.” **Armed Forces Journal International**, January 1999, v. 136, no. 6, p. 18-19.

Hardesty, David C. “Fix Net Centric for the Operators.” **United States Naval Institute Proceedings**, September 2003, v. 129, no. 9, p. 68-71.

Holland, William J., Jr. “Network Centric Warfare in ASW.” **Naval Forces**, 2001, v. 22, no. 5, p. 8+

Holzer, Robert. “Navy Speeds Toward Centralized Information System.” **Navy Times**, November 24, 1997, v. 47, no. 7, p. 35.

_____. “Navy to Establish ‘Network Centric’ Center.” **Navy Times**, November 22, 1999, v. 49, no. 7, p. 21.

_____. “Network to Make Information As a Weapon.” **Navy Times**, March 17, 1997, v. 46, no. 24, p. 32.

_____. “A New Way to Play the Game.” **Navy Times**, August 11, 1997, v. 46, no. 45, p. 16.

Hughes, David. “Net-Centric War's Focus Should Be Counter-Terrorism.” **Aviation Week & Space Technology**, December 16, 2002, v. 157, no. 25, p. 55-58.

Isby, David C. and Timothy Biggs. “Enabling Defense Transformation: Network-Centric Warfare and Ballistic Missile Defense.” **Comparative Strategy**, October-November 2003, v. 22, no. 4, p. 325-334.

Jenik, Douglas A. and Martin F. Schaffer. “Beyond the Rose-Colored Glasses.” **United States Naval Institute Proceedings**. February 2000, v. 126, no. 2, p. 60-63

Jewett, Charles and David Narkevivius. “A Synergistic Increase in Combat Capabilities – NAVAIR (Naval Air Systems Command): Shaping the Air Node for NCW (Network Centric Warfare).” **Sea Power**, March 1999, v. 42, no. 3, p. 43-44.

Keeter, Hunter C. “Network Centric Warfare.” **Sea Power**, March 2004, v. 48, no. 3, p. 12-14.

_____. “Network Centric Warfare: Aims to Translate Information Superiority into Combat Advantage.” **Sea Power**, March 2004, v. 47, no. 3, p. 12-14.

_____. “Pervasive Sensing Holds the Key to Network Centric Warfare.” **Sea Power**, September 2004, v. 47, no. 9, p. 9-11.

Kumble, Stephen. “Asia Eyes UAVs as Path to C4ISR and Network Centric Warfare.” **Asian Defence Journal**, November 2004, no. 11, p. 32-34+

Ladymon, Joseph M. “Network-Centric Warfare and Its Function in the Realm of Interoperability.” **Defense Acquisition Review Journal**, Spring-Summer 2001, v. 8, no. 2, p. 111-119.
http://www.dau.mil/pubs/arq/2001arq/ladymon.pdf

Langley, James A.G. “Network-Centric Warfare: An Exchange Officer's Perspective.” **Military Review**, November/December 2004, v. 84, no. 6, p. 47-52.
http://usacac.army.mil/cac/milreview/download/English/NovDec04/langley.pdf

Lawlor, Maryann. “Engineering Network-Centric Warfare.” **Signal**, August 2007, v. 61, no. 12, p. 23-27.

Leopold, George. “Nets: DOD's First Line of Defense.” **Electronic Engineering Times**, October 13, 1997, n. 975, p. 1-2.

Lescher, William K. “Network-Centric: Is it Worth the Risk?” **United States Naval Institute Proceedings**, July 1999, v. 125, no. 7, p. 58-63.

Marchant, Susan. “Toolkit Empowers Warfighers for Net-Centric Warfare.” **Military Intelligence**, July-September 2007, Volume 33 Number 3. http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=592&issueID=46

Mitchell, Paul T. “Small Navies and Network-Centric Warfare: Is there a Role?” **Naval War College Review**, Spring 2003, v. 56, no. 2, p. 83-99.

Moon, Terry. “Net-Centric or Networked Military Operations?” **Defense & Security Analysis**, March 2007, v. 23, no. 1, p. 55-67.

Murdock, Paul. “Principles of War on the Network-Centric Battlefield: Mass and Economy of Force.” **Parameters**, Spring 2002, v. 32, no. 1, p. 86+ *http://www.carlisle.army.mil/usawc/Parameters/02spring/murdock.htm*

Nathman, John. “Naval Aviation: The Key Enabler.” **Naval Aviation News**, May/June 1999, v. 81, no. 4, p. 2-3.

_____. “Revolution in Naval Aviation.” **Naval Aviation News**, January/February 1999, v. 81, no. 2, p. 2-3.

“Naval Air Systems Command: One Team.” **Naval Aviation News**, January/February 1999, v. 81, no. 2, p. 12-13.

“Netwar Across the Spectrum of Conflict.” **Studies in Conflict & Terrorism**, July-September 1999, v. 22, no. 3, Entire Issue.

“Network-Centric ASW.” **Naval Forces**, 1999, v. 20, no. 3, p. S6-S9.

“Network Centric Warfare: Real-Time Awareness.” **All Hands**, January 1998, no. 969, p. 52-53.

Nitschke, Stefan. “Network-Centric Warfare: The European Initiatives.” **Military Technology**, March 2004, v. 28, no. 3, p. 18, 21-26.

_____. “Network-Centric Warfare: The European Initiatives.” **NATO's Nations and Partners for Peace**, 2004, v. 49, no. 3, p. 168+

_____. “Submarines in NCW -- Roles and C4ISR Requirements.” **Naval Forces**, 2004, v. 25, no. 5, p. 22-24+

Nitschke, Stefan and John Martin. “Submarines in NCW – Roles and C4ISR Requirements.” **Naval Forces**, 2004, v. 25, no. 5, p. 22-24+

Olsson, Gustaf. “Defensive Aids Systems in Network Centric Warfare: Prospects and Possibilities.” **Military Technology**, June 2004, v. 28, no. 6, p. 70+

Phister, Paul W., Jr. “Command and Control Implications of Network-Centric Warfare.” **AFRL Technology Horizons**, February 2005, v. 11, no. 4.

Podlesny, Robert L. “Infrastructure Networks are Key Vulnerabilities.” **United States Naval Institute Proceedings**, February 1999, v. 125, no. 2, p. 51-53.

Raskin, A.V. and V.S. Pelyak. “On Network-Centric Warfare.” **Military Thought**, 2005, v. 14, no. 2, p. 86-92.

Rathmell, Andrew. “Netwar in the Gulf.” **Jane's Intelligence Review**, January 1997, v. 9, no. 1, p. 29-32.

Rehnstrom, Folke. “Moving Towards Network Centric Warfare.” **Military Technology**, August 2002, v. 26, no. 8, p. S11-S12.

_____. “Net Centric Warfare-The Swedish Viewpoint.” **NATO's Nations and Partners for Peace**, 2003, v. 48, no. 2, p. 103,106.

Reid, Darryn F., Graham Goodman, Wayne Johnson and Ralph E. Giffin. “All That Glisters: Is Network-Centric Warfare Really Scientific?” **Defense & Security Analysis**, December 2005, v. 21, no. 4, p. 335-367.

Rhodes, John E. “Network Centric Works for Marines.” **United States Naval Institute Proceedings**, September 1998, v. 124, no. 9, p. 2.

Richardson, Doug. ”Network-Centric Warfare: Revolution of Passing Fad?” **Armada International**, October/November 2004, v. 28, no. 5, p. 62+

Ronfeldt, David. “Netwar Across the Spectrum of Conflict: An Introductory Comment.” **Studies in Conflict & Terrorism**, July-September 1999, v. 22, no. 3, p. 189-192.

Robinson, Clarence A., Jr. “Network-Centric Warfare Beckons Decision Makers.” **Signal**, May 1998, v. 52, no. 9, p. 53-58.

Rubel, Robert C. “War-Gaming Network-Centric Warfare.” **Naval War College Review**, Spring 2001, v. 54, no. 2, p. 61-74.

Ryan, Michael. “Finding Alligators: The Future of Network-Centric Warfare.” **Australian Army Journal**, Autumn 2005, v. 2, no. 2, p. 101-122. *http://www.defence.gov.au/army/lwsc/Publications/journal/AAJ_Autumn05/AAJ_Autumn05_ryan_12.pdf*

Scarborough, Sheila. “Network-Centric Warfare Meets the Laws of the Navy.” **United States Naval Institute Proceedings**, May 2001, v. 127, no. 5, p. 30-33.

Schaar, David. “Identifying Essential Technologies for Network-Centric Warfare.” **CrossTalk: Journal of Defense Software Engineering,** September 2004, v. 17, no. 9, p. 26-29. *http://www.stsc.hill.af.mil/crosstalk/2004/09/0409Schaar.pdf*

Schmidtchen, David. “Network-Centric Warfare: An Idea in Good Currency.” **Australian Army Journal**, Autumn 2005, v. 2, no. 2, p. 111-123. *http://www.defence.gov.au/army/lwsc/Publications/journal/AAJ_Autumn05/AAJ_Autumn05_schmidtchen_13.pdf*

Scott, William B. "CINCSPACE Wrestles with Network Defense." **Aviation Week & Space Technology**, November 15, 1999, v. 151, no. 20, p. 93.

Sherman, Jason. “The Secrets of Centric.” **Sea Power**, April 2005, v. 48, no. 4, p. 16-18.

Shufird, Jacob L. “Tomorrow’s Sea Power Plays Today.” **United States Naval Institute Proceedings**, January 2000, v. 126, no. 1, p. 32-35.

Smith, Edward A., Jr. “Network-Centric Warfare: What’s the Point?” **Naval War College Review**, Winter 2001, v. 54, no.1, p. 59-75.

Springett, John P., II. “Network Centric War Without Art.” **United States Naval Institute Proceedings**, February 2004, v. 130, no. 2, p. 58-61.

Stillman, Patrick M. “Debate & Response: Small Navies Do Have a Place in Network-Centric Warfare.” **Naval War College Review**, Winter 2004, v. 57, no. 1, p. 94-101.

“Submarines and Network-Centric Warfare.” **Sea Technology**, September 1998, v. 39, no. 9, p. 78-79.

Tirpak, John A. “The Network Way of War.” **Air Force Magazine**, March 2005, v. 88, no. 3, p. 26-31.

Vergun, David. "An Incredible Level of Situational Awareness." **Sea Power**, October 2001, v. 44, no. 10, p. 54-57.

Walsh, Edward J. “Exercise Demonstrates Benefits of Military's Network-Centric Warfare.” **Signal**, November 1997, v. 52, no. 3, p. 16-21.

Wathen, Alex. “Joint Airspace Management and Deconfliction: A Chance to Trade in a Stovepipe for Network-Centric Warfare.” **Air & Space Power Journal**, Fall 2006, v. 20, no. 3, p. 26-34.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj06/fal06/wathen.html

West, Leslie. “Exploiting the Information Revolution: Network-Centric Warfare Realizes Its Promise.” **Sea Power**, March 1998, v. 41, no. 3, p. 38-40.

Wilson, J. R. “Network Centric Warfare Marks the Frontier of the 21st Century Battlefield.” **Military & Aerospace Electronics**, January 2000, v. 11, no. 1, p. 13-16.

Whitman, Edward C. “Submarines in Network Centric Warfare.” **Sea Power**, July 1999, v. 42, no. 7, p. 33-36.

Wise, G.J. “Network Centric Warfare: Evolution or Revolution?” **Royal Air Force Air Power Review**, Winter 2002, v. 5, no. 4, p. 64-85.

Wolthusen, Stephen D. “Self-Inflicted Vulnerabilities.” **Naval War College Review**, Summer/Autumn 2004, v. 57, no. 3/4, p. 103-113.
http://www.nwc.navy.mil/press/review/documents/NWCRSU_A04.pdf

Woodcock, William A. “Joint Forces Air Command Problem: Is Network-Centric Warfare the Answer?” **Naval War College Review**, Winter 2003, v. 56, no. 1, p. 124-138.

Wright, Richard L. “Advantage Navy [Impact of Network-Centric Warfare – Information Superiority].” **Surface Warfare**, November-December 1997, v. 22, no. 6, p. 7-9.

Zanini, Michele. “Middle Eastern Terrorism and Netwar.” **Studies in Conflict & Terrorism**, July-September 1999, v. 22, no. 3, p. 247-256.

Zimm, Alan. “Human-Centric Warfare.” **United States Naval Institute Proceedings**, May 1999, v. 125, no. 5, p. 28-31.

Documents, Theses & Technical Reports

Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography.

Alme, Thorsten. ***Interoperability and Network-Centric Warfare: US Army Future Force and German Army in 2015***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2005. 77p.

Abstract: U.S. and German security strategies portray future warfare as coalition warfare. Thus, successful military operations will depend on the assured interoperability of coalition forces. This paper examines the state of interoperability between German Forces and the U.S. Army Future Force in 2015. The author describes the U.S. Future Force, whose characteristics and influence on foreign nations' interoperability are evaluated. Special consideration is given to technical and behavioral interoperability. The monograph also assesses the projected capabilities of the German Bundeswehr in the year 2015 with regard to Network-Centric Warfare (NCW). Technical and behavioral interoperability are again the main focus. According to the findings of the paper, German Bundeswehr forces in 2015 will be prepared for integration into the U.S. Army Future Force. The single most important factor for assuring this integration will be appropriate military funding in the next 10 years.

ACCESSION NUMBER: ADA437452

http://handle.dtic.mil/100.2/ADA437452

Amir, Yair. ***Scalability, Accountability and Instant Information Access for Network-Centric Warfare.*** Baltimore, MD: Johns Hopkins University, 2006. 55p.

Abstract: This project focused on one main problem: How to scale intrusion tolerant replication to wide area networks while considerably improving performance. During the last few years, there has been considerable progress in the design of intrusion-tolerant (Byzantine) replication systems. The state of the art before this project performed well on small scale systems that were usually confined to local area networks. The project developed the first hierarchical Byzantine replication architecture tailored to systems that span multiple wide area sites, each consisting of several replicas. The new architecture dramatically improves system performance (latency and throughput), availability, and manageability, for the price of extra hardware. Steward, a complete implementation of our architecture met and exceeded all performance goals and was able to withstand a white-box red team attack without being compromised even once. A side goal for the project was to look at the problem of malicious insider clients. Instead of compromising a system, malicious clients can just inject bad (but valid and authenticated) updates that corrupt information and propagate through the replicated system. By constructing an Accountability Graph between causally related updates, we demonstrate how enforcing accountability for client updates enables backtracking and state regeneration once corrupted data is discovered.

ACCESSION NUMBER: ADA454931

http://handle.dtic.mil/100.2/ADA454931

Bailey, Alvin L. ***Implications of Network Centric Warfare***. Carlisle Barracks, PA: Army War College, 204. 28p.

Abstract: This paper will examine Network Centric Warfare the centerpiece of Transformation. This form of warfare depends heavily on computer networks the Internet communications and sensors. These areas of dependence also provide numerous vulnerabilities. This paper will focus specifically on Network Centric Warfare's vulnerabilities in terms of sensors cyberterrorism/ Electro-Magnetic Pulse (EMP) and bandwidth/ frequency. The assessment of the areas listed above and the other strategic implications will lead to a conclusion as to its efficacy of Network Centric Warfare as the centerpiece of Transformation

ACCESSION NUMBER: ADA423336
http://handle.dtic.mil/100.2/ADA423336

Baker, Matthew E. ***Human Factors in Network Centric Warfare***. Newport, RI: Naval War College, 2002. 31p.

Abstract: The speed of information transfer in Network Centric Warfare is rapidly out pacing the capability to absorb and act effectively. Numerous problems, such as micro-management and limited endurance have been documented in studies of human interaction in information systems. Many of these problems are the result of limited human cognitive capability in the face of the massive amounts of information provided in NCW. Specifically, the operational level of warfare, commanders are being overwhelmed due to human factors, limitations and tendencies.

ACCESSION NUMBER: ADA405862
http://handle.dtic.mil/100.2/ADA405862

Barksdale, Carl A. ***The Network Centric Operations - Effects Based Operations Marriage: Can It Enable Prediction of "Higher Order" Effects on the Will of the Adversary***. Newport, RI: Naval War College, 2002. 24p.

Abstract: Network Centric Operations is touted as enabling Effects Based Operations targeted at the 'will and belief systems' of the adversary. This assertion is explored. Specifically, for Effects-Based Operations against the will and belief systems to be enabled, the operational commander needs to know what makes an adversary give up and needs to be able to plan and assess the associated indicators of the desired operational effect? Assessment implies measurement or sensing. The will and belief systems are psychological factors that have defied measurement or assessment. Historical analysis is conducted for three losing side's reactions to identify any patterns that may be used as measures or as indicators that desired effects have been achieved. Effects-Based Operations is a good theoretical approach to targeting and operational planning. It answers the question, Why are we taking this action? However, since the will and belief systems of the adversary are psychological factors, this paper shows that planning for higher order effects remains problematic. Thus, the operational commander will still have to rely on his/her gut fuel and occasional fleeting indicators to discern higher order effects on the will of the adversary vice plan and confirm effects via the promised in-depth knowledge provided by the omnipresent sensor grid in Network Centric Operations.

ACCESSION NUMBER: ADA405867
http://handle.dtic.mil/100.2/ADA405867

Barton, Keith W. ***Leveraging Information Technology to Enable Network Centric Engineer Reconnaissance Operations***. Cambridge, MA: Massachusetts Institute of Technology, 2003. 102p.

Abstract: The Naval Construction Force has traditionally depended on outside sources to obtain and analyze engineering data in contingency situations. The Navy has embarked on an initiative to develop Seabee Engineer Reconnaissance Teams to perform this function, both as a basis for projects slated for in-house construction and as a product to deliver to other organizations. Exercises and operations have thus far shown that the concept is viable, but Seabee Engineer Reconnaissance Teams have encountered problems with data gathering and reporting, and transmission of data and images. Concurrently, the Department of Defense is pursuing a transformation toward network- centric warfare. Network Centric Warfare represents a powerful set of warfighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information in order to bring all available assets to bear in a rapid and flexible manner. This research explores the state of the practice of military engineer reconnaissance as described by established Army doctrine and as enacted by Navy Seabee Engineer Reconnaissance Teams. Commercial information technology applications are reviewed in the areas of geographic information systems, collaborative design, and wireless communications. Solutions are proposed for their potential to enable network centric engineer reconnaissance operations.

ACCESSION NUMBER: ADA415843

http://handle.dtic.mil/100.2/ADA415843

Berger, Alexander. ***Organizational Innovation and Redesign in the Information Age: The Drug War, Netwar, and Other Lower-End Conflict***. Monterey, CA: Naval Postgraduate School, March 1998. 209p.

Abstract: The end of the Cold War and the rise of the Information Age have fostered an uncertain security environment which the United States is struggling to master. The purpose of this thesis is to explore the factors that lead complex organizations to initiate large-scale structural change in the face of environmental uncertainty; and more specifically to determine how the rise of the Information Age may change the organizational requirements of the U.S. national security structure. This thesis creates a unique framework for analysis, blending principles of organization and innovation theory with the theory of information-based netwar. This study analyzes the organizational structures adopted by several transnational drug cartels, and compares them to that of U.S. counternarcotics forces. Next, this thesis reviews a series of recent occurrences pertaining to national security to test whether there are manifestations of netwar threats emerging, and whether new and old organizational actors are learning to adapt their structures to gain an advantage over the United States. Finally, this thesis is both predictive and prescriptive with regard to the issues of organizational redesign. It argues that structural changes are necessary for the United States to ensure the national security in an Information Age. Then it makes recommendations that would help the U.S. security structure redesign itself to become more agile in the face of Information Age threats.

ACCESSION NUMBER: ADA346073

http://handle.dtic.mil/100.2/ADA346073

Berglund, Jan. ***Network Centric Warfare: A Realistic Defense Alternative for Smaller Nations?*** Monterey, CA: Naval Postgraduate School, 2004. 160p.

Abstract: This thesis establishes an analytical framework for identifying and discussing strategic factors considered important when implementing Network Centric Warfare (NCW) as a new warfighting concept for the information age. Although the findings have a broad application, the focus is on NCW implementation in the NATO Alliance's small countries, and in Norway in particular. A key question is if the emerging NCW concept is a feasible defense alternative for smaller nations. Central to the study are factors found in the strategic environment, such as Norway's strategic freedom of maneuver, its affiliation with NATO, the impact of national interests, economic and technological assumptions, and the cultural premises that underlie the power of information. The changing features in the nature of conflict and in future potential opponents also will influence NCW mission challenges, opportunities, and constraints. A particularly important mission challenge is the neglected military view of low-intensity conflicts as "worthy" military missions as well as the sociological impact on networked actors and opponents, as conditioned by new trends in the information age. A key finding is that NCW, which also takes into consideration the impact of other strategic factors discussed in this thesis, has the potential to rise to the many challenges and achieve many of the objectives currently "floating" in existing military transformation strategies.

ACCESSION NUMBER: ADA424706

http://handle.dtic.mil/100.2/ADA424706

http://bosun.nps.edu/uhtbin/hyperion-image.exe/04Jun%5FBerglund.pdf

Blatt, Nicole I. ***Trust and Influence in the Information Age: Operational Requirements for Network Centric Warfare.*** Monterey, CA: Naval Postgraduate School, 2004. 113p.

Abstract: Military leaders and scholars alike debate the existence of a revolution in military affairs (RMA) based on information technology. This thesis will show that the Information RMA not only exists, but will also reshape how we plan, operate, educate, organize, train, and equip forces for the 21st century. This thesis introduces the Communication Technology (CommTech) Model to explain how communication technologies affect organizations, leadership styles, and decision-making processes. Due to the growth in networking enterprises, leaders will have to relinquish their tight, centralized control over subordinates.

Instead, they will have to perfect their use of softer power skills such as influence and trust as they embrace decentralized decision-making. Network Centric Warfare, Self-Synchronization, and Network Enabled Operations are concepts that provide the framework for integrating information technology into the battlespace. The debate that drives centralized versus decentralized control in network operations is analyzed with respect to the CommTech Model. A new term called Operational Trust is introduced and developed, identifying ways to make it easier to build trust among network entities. Finally, the thesis focuses on what leaders need to do to shape network culture for effective operations.

ACCESSION NUMBER: ADA429673

http://handle.dtic.mil/100.2/ADA429673

http://bosun.nps.edu/uhtbin/hyperion-image.exe/04Dec%5FBlatt.pdf

Borchert, R. Alistair. ***Organizational Fitness of a Proposed Network Centric Organization***. Monterey, CA: Naval Postgraduate School, December 1998. 149p.

Abstract: Network Centric Warfare (NCW) capitalizes on technology to obtain and maintain an enhanced situational awareness and uses the distributed offensive firepower of the collective force to fight the battle. Speed of Command and Self- Synchronization are key tenants of NCW. The author proposes an organization designed to operate in the NCW environment. It consists of the Force Commander and commanders of Situational Awareness, Resources, Effects, and Operations. The research question of this thesis is whether or not the proposed organization is fit in the NCW environment. The organization is looked at in two 'snapshots': one is the planning process and the other is the execution process. The expert system Organizational Consultant is used to analyze the organization and determine its organizational fitness. The results indicate that the proposed organization is fit if changes are made to make the planning process highly centralized and the execution process decentralized. Formalization will also need to be lowered in the organization.

ACCESSION NUMBER: ADA358976

http://handle.dtic.mil/100.2/ADA358976

Braunlinger, Thomas K. ***Network Centric Warfare Implementation and Assessment***. Fort Leavenworth, KS: Army Command and General Staff College, 2005. 88p.

Abstract: This study examines three primary questions: (1) What is the definition of network-centric warfare?, (2) Are the military services implementing the network-centric warfare concept?, and (3) Is the network-centric warfare concept a new theory of warfare or rather a modification or extension of previous theories? To answer these questions, various publications on network-centric warfare and the various military service transformation plans were reviewed. The definition of network-centric warfare developed is the linkage of people, systems, and platforms to form a self-synchronized networked force that creates shared battlespace awareness for information superiority and speed of command. A review of the services transformation plans showed that the services may not be using the same terms, but they are implementing the concepts of network-centric warfare. The study concludes that network-centric warfare is not a new theory of warfare, but a concept that supports the maneuver theory of warfare, similar to the concept of blitzkrieg developed by Germany prior to World War II. To emphasize this the term "network-enabled warfare" is suggested as a more appropriate term.

ACCESSION NUMBER: ADA436488

http://handle.dtic.mil/100.2/ADA436488

Brown, Michael A. ***Implications of Outsourcing on Network Centric Warfare***. Carlisle Barracks, PA: Army War College, 2002. 29p.

Abstract: The Department of Defense (DoD) has taken about 80 percent of the government cutbacks since the end of the Cold Wan As a means to fashion cost savings and gain efficiencies, DoD is seeking to streamline much of its infrastructure. One popular idea to assist in the streamlining effort is through the outsourcing of Information Technology (IT) functions. There is a sentiment within the Department of the Army (DA) that the entire Information Management/information Systems element of the Army can be outsourced without having an impact to the Army. The purpose of this research paper is to examine this

sentiment to determine if it makes sense or where it could create problems as the Army moves towards a network centric warfare environment. It will examine the Army's IT requirements to support network centric warfare, examine potential outsourcing options, and determine the implications of these options to the effectiveness of achieving the requirements.
ACCESSION NUMBER: ADA401884
http://handle.dtic.mil/100.2/ADA401884

Caneva, Joseph W. ***Network-Centric Warfare: Implications for Applying the Principles of War.*** Newport RI: Naval War College, Joint Military Operations Department, May 1999. 25p.
Abstract: Noting the competitive advantage that a computer network system completely integrated into a firm's structure and operations has provided to businesses, individuals have begun to argue that adoption of this concept by the United States armed forces would produce a comparable, competitive advantage in warfare. This concept, "network-centric warfare," a vision of warfare focused upon the central importance of a network of sensors, platforms, weapons, and users and its resulting synergistic effect, is beginning to cause considerable debate among those interested in the future of America's armed forces. Advocates of the network-centric concept of warfare foresee that it will provide a clear, detailed picture of the battlespace, increased speed of command, self- synchronization of units, and increased ability to mass effects. These enhanced capabilities, if ultimately realized, obviously have the potential to affect the manner in which commanders conduct war at the operational level. The paper's intent is to take the anticipated benefits of network-centric warfare as givens and then to examine the implications of these capabilities in applying the principles of war at the operational level of warfare.
ACCESSION NUMBER: ADA372759
http://handle.dtic.mil/100.2/ADA372759

Carr, James. ***Network Centric Coalitions: Pull, Pass, or Plug-In?*** Newport, RI: Naval War College, May 1999. 25p.
Abstract: The author traces the evolution of Network Centric Warfare, showing its American roots. He shows that NCW is not a remote concept on the horizon, it is nascent in today's maritime operations and inevitably will be the way in which the U.S. Navy will fight future wars. Then he reveals a gaping mismatch between the emerging operational doctrine and the strategy it will be tasked to support. Since it is largely an American conception for warfare, the United States thus bears the burden to pursue interoperability with regional coalition partners if it is to fight 'together when we can, alone if we must'. Finally, the author presents options for addressing this strategic/operational mismatch and proposes a way ahead.
ACCESSION NUMBER: ADA370694
http://handle.dtic.mil/100.2/ADA370694

Carr, Timothy D. ***Network-Centric Warfare: Are We Past the Age of De-centralized Execution?*** Newport, RI: Naval War College, 2004. 21p.
Abstract: This paper examines the validity of the concept of "Centralized Command, De-centralized Control", and offers an alternative view of Operational-level involvement in tactical execution made possible by current and developing information technology. The paper begins by citing positive examples of Centralized control during several recent tactical actions. A review of information factors necessary to provide overall battlefield situational awareness is conducted, including current and developing capabilities. Instances where Centralized control of tactical execution would not he desired are discussed, along with the requirement to retain current capabilities to operate without Centralized control of tactical actions. The scope of operations where a Joint Force Commander might become involved in tactical control is discussed with examples delivered. The current Joint Staff composition is given and a modified Joint Staff Organization is presented to help the Joint Force Commander integrate himself into tactical execution in a positive fashion. This paper questions the universal application of accepted doctrine. It asserts the value of deviating from doctrine where such deviation would work to more rapidly achieve Operational objectives. Recommendations are made regarding the composition of the typical Joint Staff in

order to take advantage of technological innovation. While technological advances provide the basis of the paper's premise, the paper is focused on Leadership and Command relationships rather than technology.

ACCESSION NUMBER: ADA422804

http://handle.dtic.mil/100.2/ADA422804

Cianciolo, Mark G. ***Network Centric Warfare: A Bridge Too Far?*** Newport, RI: Naval War College, 2003. 19p.

Abstract: Network Centric Warfare (NCW) is viewed as the bedrock of transformation and future warfighting (i.e. common operating picture flattening command and control by connecting strategic level commanders to tactical level warfighters). However the moral domain of conflict having been largely ignored by NCW advocates will in all likelihood prohibit its successful implementation at the lowest level of warfighting; the tactical level. Therefore in future conflict the author believes that it is this domain the moral domain that if not completely understood and taken into account will limit if not prevent the full potential and exploitation of Network Centric Warfare as envisioned by its advocates. This research paper is relevant to the strategic operational and tactical levels of warfare in that NCW is clearly a major pillar in the quest for transformation of United States military forces. If the human dimension is a single point of failure in Network Centric Warfare then the NCW concept needs to address this issue and identify the relationship and human interface required to successfully achieve and propel this future capability from a concept in its present form to a reality in its application.

ACCESSION NUMBER: ADA419368

http://handle.dtic.mil/100.2/ADA419368

Copley, E. C. ***A Commander in Chief's Network-Centric Odyssey***. Newport, RI: Naval War College, 2002. 26p.

Abstract: Network-Centric Operations continues to gain acceptance as a construct for future military operations. Operational Art, on the other hand, stands as a principal construct for past military successes and constitutes current joint doctrine. Some critics suggest implementing Network-Centric Operations presages the death of Operational Art. Each Armed Service has begun training and equipping its force using the tenets of Network-Centric Operations, but those forces come together for the first time under the combatant Commander-in-Chief. The CINC will have to determine how a fully networked force affects existing methods of employment to achieve operational and strategic objectives. This paper reconciles Network-Centric Operations and Operational Art by analyzing the underlying assumptions, assertions, and interrelationships. The analysis results in the conclusion that Network-Centric Operations and Operational Art are not mutually exclusive but mutually supporting constructs. In fact, a synergy appears that accomplishes strategic and operational objectives with extraordinary effectiveness. This conclusion leads to six recommendations for the Commander-in-Chief that harmonizes Network-Centric Operations and Operational Art in the theater of operations to ensure future success.

ACCESSION NUMBER: ADA400924

http://handle.dtic.mil/100.2/ADA400924

Coury, Michael J. ***The Joint Air Operations Center in the Realm of Network Centric Warfare***. Newport, RI: Naval War College, 2001. 34p.

Abstract: The concept of Network Centric Warfare (NCW) is advertised to significantly change the way the military operates in the future. The proliferation of information technology and its ability to provide for centralized control while decentralizing execution are but two foundations for these changes. Those concepts, however, are not novel. In fact, the evolution of the Joint Air Operations Center (JAOC) demonstrates a continual effort to achieve those same objectives. Unfortunately, the JAOC still falls short in achieving the expediency of execution so necessarily in modern warfare. The ability to support significantly increased operational tempo will be required not only in the JAOCts domain of airspace, but on the ground and at sea as well. Given the adherence to the manner in which the JAOC currently organizes and functions, there is only so far technology can go to improve timely and efficient execution.

With the advent of NCW, the JAOC has an opportunity to metamorphose again, achieving improvements to support vastly increased operational tempo. Limitations of organization, functions and execution can be resolved by applying the NCW concepts of shared awareness, self-synchronization and massing effect. By rethinking the current function and execution methodology of the JAOC and melding them into a Joint Operations Center (JOC) organized by capability rather than operational median, we will provide for the efficiency inherent in NCW and a more robust and high tempo at all levels of military operations.

ACCESSION NUMBER: ADA393370

http://handle.dtic.mil/100.2/ADA393370

Critchlow, Robert D. ***Weaving the Net: Linking Space Systems to Theater Operations***. Newport, RI: Naval War College, February 1998. 22p.

Abstract: Joint Vision 2010 visualizes a military in which the principle of mass is redefined. Mass in 2010 will be characterized by the massing of effects, rather than mass derived by way of a superior number of people or platforms. Information superiority, by enabling dominant battlefield awareness, is the key to achieving this redefinition. Information superiority is achieved in the military in the same way it is being achieved in the civilian sector: through a shift away from expensive and centralized platforms toward a distributed information architecture. Network centric warfare relies on a pervasive information grid that provides the nervous system that links sensors and shooters. The information grid can be achieved only through heavy reliance on space based assets. Joint forces already lean upon satellites to support their communication needs, as seen in Desert Storm. Only space based communications can meet the needs of forces deploying from CONUS to remote locations that lack indigenous communications infrastructures. It is unlikely that theater commanders will have the time to establish ground based communications in a fast moving crisis. These assets must be military, as commercial systems present limitations that will not be overcome except in the gravest of contingencies. Unfortunately, existing constraints prohibit space systems from completely fulfilling the dream of bandwidth on demand required to implement the JV2010 operational concepts. Technical limitations cap the capability of existing satellite constellations. More importantly, organizational inefficiencies hamper the joint force commander's ability to maximize support from these finite resources. Exploiting existing unified command structures, by centralizing authority to apportion MILSATCOM resources by mission need under USSPACECOM, could provide meaningful improvements.

ACCESSION NUMBER: ADA348377

http://handle.dtic.mil/100.2/ADA348377

Cummings, John J. ***Does Network Centric Warfare Equal Micromanagerial Warfare? Minimizing Micromanagement at the Operational Level of War?*** Newport, RI: Naval War College, 2003. 24p.

Abstract: Recent advances in communications, sensors, and computers have brought the U.S. military into a new age of technical transformation. This transformation has resulted in a new approach to the conduct of warfare, often referred to as network centric warfare (NCW). NCW possesses incredible potential for the lethal and efficient conduct of future wars, but it also enables a less than desirable aspect of armed conflict--leadership by micromanagement. This is a result of the capabilities inherent in NCW that cause senior leaders, unable to resist the urge to control tactical operations, to directly influence the achievement of strategic objectives. The intent of this paper is to examine micromanagement at the operational level of war, more specifically, from the national-strategic (civilian leaders) and theater-strategic/theater-operational (COCOM) level to the tactical level. Analysis from recent military operations will be conducted to develop short term and long term approaches that will minimize the effects of this ineffective leadership style.

ACCESSION NUMBER: ADA415392

http://handle.dtic.mil/100.2/ADA415392

Day, Newell B., II. ***Network Centric Warfare and the Joint Forces Air Component Commander***. Newport, RI: Naval War College, February 1999. 20p.

Abstract: The JFACC concept rests on the belief that aircraft possess a unique ability to reach the deep battle and need to be centrally controlled and coordinated. Today, however, the JFACC controls more than just aircraft. The JFACC staff continues to grow to accommodate controlling and coordinating new technologies. In reality, the ability of aircraft to reach and influence the deep battle is no longer unique. It applies to a myriad of weapons, sensors, and information. A network centric automated system is better suited to control and coordinate these assets. Such a system would be able to absorb the functions of JFACC as a subset of functions performed. The system would be far streamlined and much more efficient than the JFACC. This system is interactive and fuses all information, weapons, and sensors into a common situational picture for all users. This system is a battlespace system.

ACCESSION NUMBER: ADA363152

http://handle.dtic.mil/100.2/ADA363152

DeLange, Eric P. and Mike Morris. ***Decision-Centric Warfare: Reading Between the Lines of Network-Centric Warfare.*** Newport, RI: Naval War College, 2006. 26p.

Abstract: Network-Centric Warfare (NCW), as it has come to be called, is here to stay. While the benefits are proving to be many, there are also potential risks that can adversely affect operational leadership. Increasingly, commanders today must be aware of how the effects of information overload, instantaneous communications, and increased opportunities to insert themselves in levels of war outside their traditional sphere of influence can have a bearing on their decision-making. NCW's very name has a tendency to focus attention strictly on the technology, as if once "the system" is implemented or "the device" installed, that everything will work out for the best. The technology is merely an enabler, another addition to commanders' toolkits to help them make better decisions. To avoid the "if you build it they will come" mentality, the focus must be maintained on decision-making and the decisions that result through a commander's application of operational art. This paper proposes replacing one word and calling it Decision-Centric Warfare to maintain the proper focus. Not only does the name change align more directly with Joint Vision 2020's concept of decision superiority, but when one looks at the NCW terminology and construct, decisions are really what NCW is all about.

ACCESSION NUMBER: ADA463459

http://handle.dtic.mil/100.2/ADA463459

Diggs, D. G. ***Weapons of Mass Destruction a Network-Centered Threat***. Newport, RI: Naval War College, May 1998. 23p.

Abstract: Battlespace dominance is more than the physical control of air, land, and sea. Under the network centric concept of operations, U.S. forces must be ready to control the infosphere in order to assure military objectives can be achieved. Perhaps the most effective information warfare (IW) weapon is a Weapon of Mass Destruction (WMD), specifically a biological or nuclear weapon. Important questions should be answered about the ability to protect American information networks from the significant information disruption characteristics of WMD.

ACCESSION NUMBER: ADA351710

http://handle.dtic.mil/100.2/ADA351710

DIRusso, Lawrence R. ***Casting Our Net: Can Network Centric Warfare and Multinational Operations Coexist?*** Newport, RI: Naval War College, 2001. 20p.

Abstract: This paper is based on three assumptions: That the United States will develop Network Centric Warfare, that future military operations will involve allied and coalition partners, and that these partners will not be able to afford full implementation of network-centricity into their forces. Given these assumptions, can a Joint Task Force Commander integrate network-centric units and traditional forces and still accomplish his mission? An analysis of the basic tenets of Network-Centric Warfare (shared awareness, speed of command, self-synchronization, greater lethality, and increased survivability) indicates they are compatible with multinational operations. Through proper force allocation, mission

assignment, procedural considerations, and technological adaptations, a Joint Task Force Commander will be well served by an integrated force that can meet the required objectives.

ACCESSION NUMBER: ADA389591

http://handle.dtic.mil/100.2/ADA389591

Donnelly, Michael P. ***The First Salvo: Implications of Standing Rules of Engagement for U.S. Forces in Network-Centric Warfare***. Newport, RI: Naval War College, 2002. 29p.

Abstract: Network-centric warfare (NCW) will create distinct advantages in the operational factors of space, time, force, and their interrelationships. Information superiority, the capability for cooperatively engaged precision effects, and a responsive command and control architecture will enable commanders operating in NCW to preempt enemy forces, negating an adversary's options before they can be executed. Though the technical challenges in NCW are significant, they are incrementally proving surmountable through war gaming and experimentation. The true limit of NCW's operational capability however, may not be technology, but law and politics. Standing Rules of Engagement for U.S. Forces provides the base-line guidance and authorization for the use of military force in concert with international law and national policy. This paper examines the implications for NCW under Standing Rules of Engagement for self-defense, revealing several potential vulnerabilities and ambiguities that could significantly impact its operational capability. Operational concepts, structure, doctrine, and planning must anticipate the reality that military operations will be constrained by law and political imperatives. Though NCW provides unprecedented levels of battlespace knowledge and speed of command, the initiative that it avails U.S. forces could be significantly undermined if it fails to adequately coalesce with rules of engagement (ROE).

ACCESSION NUMBER: ADA400936

http://handle.dtic.mil/100.2/ADA400936

Eisen, Stefan, Jr. ***Network Warfare. It's Not Just for Hackers Anymore***. Newport, RI: Naval War College, Joint Military Operations Department, June 1995. 27p.

Abstract: Network warfare (Netwar) is the latest tool in the Information warfare toolbox. Where C2W targets the enemy's military electronic spectrum and provides defense against enemy C2W efforts, Netwar targets enemy computer networks that support both military and civilian functions (such as communications, logistics, transportation, and other computer controlled networks) in order to provide the operational commander with an additional tool to either prevent or win conflicts. Netwar also has defensive features, helping the operational commander defend against the inevitable enemy attack on friendly computer network systems.

ACCESSION NUMBER: ADA297897

http://handle.dtic.mil/100.2/ADA297897

Erb, Stephen S. ***Network Centric Warfare: An Operational Perspective***. Newport, RI: Naval War College, 2004. 37p.

Abstract: Network Centric Warfare development is currently proceeding from the tactical level up, with little concern to the overarching requirements of the operational level of war. The implied assumption is that the concepts, both technical and organizational, will naturally scale to the operational and strategic levels. Absent an operational perspective, what is likely to develop is a large-scale tactical tool set and an operational staff structure that evolves to support this tactical tool set. This paper examines Network Centric Warfare from the Operational Commander's perspective by first examining the Operational Commander's requirements of a command and control system, comparing those requirements to what Network Centric Warfare as currently envisioned will provide, then recommends an operational staff organization to support the requirements of the Operational Commander in a Network Centric Warfare environment. The recommended staff structure is designed to provide the Operational Commander the flexibility to benefit from self-synchronized forces as well as to take close control of forces when required by the mission.

ACCESSION NUMBER: ADA422795
http://handle.dtic.mil/100.2/ADA422795

Erbetta, John. ***Attrition in Network Centric Warfare***. Malvern, UK: Defence Science and Technology Laboratory, 2003. 17p.

Abstract: Network Centric Warfare (NCW) is concerned with exploiting information to maximize combat power. Integration of C2 systems is able to increase military effectiveness, whether in maneuver, engagement, logistics, or protection. However, this increases the potential length of the electronic chain from sensor to shooter. This paper acknowledges that battle damage and force attrition (both equipment and human) occur in real conflict. The hypothesis is that at some point this may result in decreased force effectiveness rather than increased advantage. Information warfare means that positive attacks on systems themselves compound the problem. Emerging technologies applicable to NCW as a force multiplier need to be recognized as counter to the impediments to progress in the development of NCW. The impact of battle damage, attrition, and cyber attack is addressed as well as system security and the associated human factors of authority and responsibility. Options to minimize these vulnerabilities are postulated. The development of distributed systems and the potential of using arbitration in decision making is viewed as one way to minimize the impact of performance on C2 effectiveness. The paper also recognizes that while dominance (in its widest sense) is the ambition of symmetric warfare, in the asymmetric case structures can be undermined by relatively unsophisticated attack. In particular, the paper's purpose is to underline the fact that implementations need to ensure that attrition results in graceful, rather than catastrophic, degradation. At the extreme end of the C2 performance spectrum the following question must be asked: To what extent can degraded C2 performance threaten force effectiveness? Assessment at this level is difficult and real answers are only likely to come from real-life exercises that study the degree of reliance on C2 effectiveness during battle. The output will indicate that steps that need to be taken.

ACCESSION NUIMBER: ADA425258
http://handle.dtic.mil/100.2/ADA425258

Erdie, Philip B. ***Network-Centric Strategic-Level Deception***. Monterey, CA: Naval Postgraduate School, 2004. 49p.

Abstract: This thesis explores strategic-level deception in the context of network-centric information operations. Advances in information technology and the global connectedness of communications networks have created new opportunities and challenges for conducting strategic and operational level deception campaigns with significant utilization of cyberspace. Planning and executing concurrent strategic-level deceptions among distributed participants and against multiple targets requires speed, flexibility, and situational awareness. This thesis begins with a historical account of twentieth century use of strategic-level deception, followed by a definition of network deception, considerations for achieving network-based deception, and our proposed model of command structure for network-centric planning and execution of deception campaigns in the twenty-first century.

ACCESSION NUMBER: ADA427121
http://handle.dtic.mil/100.2/ADA427121
http://bosun.nps.edu/uhtbin/hyperion-image.exe/04Sep%5FErdie.pdf

Farmen, Stephen E. ***Network Centric (NETCENTRIC) Warfare (NCW): A LOGCENTRIC Perspective***. Newport, RI: Naval War College, 2001. 25p.

Abstract: As the concept of Network Centric (NETCENTRIC) Warfare (NCW) evolves to produce what many experts and military professionals view as a Revolution in Military Affairs (RMA), it would be both wise and prudent for the U.S. military to consider a simultaneous Logistics Centric (LOGCENTRIC) approach to better harness our efforts for near-term gain and prepare for long-term benefit. This may affect a boost in combat power immediately and, more importantly, allow us to form a responsive logistics architecture relevant to a giant leap into NCW, Joint Vision 2010/20, and a SMA we can control and use to our advantage. NCW and the RMA it suggests will be ineffective if we let enthusiasm for its potential

outdistance our capability to support its inception and diminish the combat power it was intended to increase. We must use the current inter-conflict period to build a forward-looking logistics architecture that nurtures NCW to make its promise of increased combat power a reality. If one has a concept but lacks precise requirements, one is best served by building capability to determine the endstate, not vice versa. A LOGCENTRIC approach to NETCENTRIC warfare supports this theory. Only with a LOGCENTRIC approach to NCW can we meter this concept to life in a positive manner. Thus, a LOGCENTRIC approach to NETCENTRIC warfare is a more prudent way to ensure a smooth road ahead as we evolve in the 21st century.

ACCESSION NUMBER: ADA389710

http://handle.dtic.mil/100.2/ADA389710

Fewell, M. P. and Mark G. Hazen. ***Network-Centric Warfare-Its Nature and Modelling.*** Salisbury, Australia: Defence Science and Technology Organisation, Systems Sciences Laboratory, 2003. 67p.

Abstract: This study examines the concept of network-centric warfare with the aims of characterising network centricity as clearly as possible and identifying metrics for level of net-centricity'. Properties of network-centric systems, as expounded in the literature, were critically examined to derive examples of suitable metrics. This examination suggests that, except for the provision of reachback, none of the properties is clearly diagnostic of network centricity: it is possible to conceive of systems displaying one or more of them despite not being net-centric as we understand the term. This means that metrics for these properties are not well correlated with the degree of network centricity of the system. Another list of properties was compiled, derived from characteristics of the internet and other effective networks, that is better suited to the identification of network centricity. Consideration of this led to the conclusion that access to a high-capability network is not sufficient for a system to be network-centric, it is also necessary that the network be used in an appropriate manner-a manner supporting the force as a whole, rather than being focused on the needs of a particular unit or platform. Not only must the right information be available to the right person at the right time in the right form, but also it must be put to the right use. This emphasis on motivation in the definition of network centricity parallels, though is distinct from, recent work emphasizing human aspects in command and control (C2). As with C2, network centricity is not just about hardware. The question of defining a general metric that faithfully indicates level of network centricity is examined with the aid of a specific example, but remains open.

ACCESSION NUMBER: ADA420257

http://handle.dtic.mil/100.2/ADA420257

Finnegan, Richard J. ***Organizational Implications of Network-Centric Warfare***. Newport, RI: Naval War College, February 1999. 25p.

Abstract: One of the many proposed responses to the rapidly changing global environment and significant fiscal constraints at the onset of the information age has been the concept of network centric warfare. The proponents of the concept draw support from successes achieved by high tech segments of the business world that have embraced advances in information technology. At issue is not whether or not the Navy (and other services) will seek to exploit information technology to the fullest extent possible. Indeed examples of the Navy's quest to distribute information in a graphic network format actually predate the end of the Cold War by decades. What is controversial is the extent to which the introduction of advanced information technology will change the hierarchical system of human interaction that has dominated successful military organizations for thousands of years. Before we decide our course we must examine the likely political realities of tomorrow's conflicts, the characteristics of current versus proposed force profiles and most importantly the influence of today's business practices on military affairs.

ACCESSION NUMBER: ADA363092

http://handle.dtic.mil/100.2/ADA363092

Garth, Dennis. ***Network Centric Warfare and Its Impact on Operational Functions***. Newport, RI: Naval War College, 2003. 23p.

Abstract: Network-Centric Warfare (NCW), or Network-Centric Operations (NCO), is a term that evokes strong opinions. The proponents of NCW look to the future and see sensor grids, weapons platforms netted together, and the free flow of information relating the minute details of friendly and enemy forces. The opponents of NCW claim that the ability of net centric operations to give the commander detailed information about the battlespace will flatten the command hierarchy and tempt operational commanders to dabble in tactical decisions rather than concentrating on operational art. The use of Net-centric tools in modern warfare has not hampered warfighting. On the contrary, they have provided the synthesis of information needed to conduct operations, greatly enhancing the warfighting capability of the modern commander. For NCW to mature from the current tactical to the future operational level, it must support the operational commander and his/her staff in the functions of operational art. NCW as it exists today and in the near future can provide the Operational Commander with the tools to plan, collaborate and increase the speed with which the staff perform. It is through NCW that the Operational Commander will react quicker there-by shocking the adversary or thwarting an enemy timetable for victory. Net centric warfare will, in the future, bring these about.

ACCESSION NUMBER: ADA415477

http://handle.dtic.mil/100.2/ADA415477

Geraghty, Barbara A. ***Will Network-Centric Warfare be the Death Knell for Allied/Coalition Operations?*** Newport, RI: Naval War College, May 1999. 25p.

Abstract: The U.S. Navy is undergoing a shift in its focus from platform-centric to network-centric warfare in the coming century. Enabled by the recent advances in information technology, network-centric warfare connects widely dispersed platforms into a robust network capable of massing tremendous effects. Network-centric warfare will challenge the operational commander when planning allied /coalition operations in two major areas. The first is interoperability, which includes issues of technology compatibility, intelligence sharing, classified material security policy, language, and rules of engagement. The second challenge addresses the issue of command and control, specifically as national culture and subordination of forces affect it. The operational commander must determine the ability of coalition partner forces to be part of the network and assign mission tasks accordingly. As history has shown, coalition operations require significant leadership on the part of the commander and network-centric warfare is simply another factor to add to the challenge.

ACCESSION NUMBER: ADA370700

http://handle.dtic.mil/100.2/ADA370700

Ginter, Karl. ***Space Technology and Network Centric Warfare: A Strategic Paradox.*** Carlisle Barracks, PA: Army War College, 2007. 22p.

Abstract: The Department of Defense (DoD) force transformation is in large measure predicated on harnessing and exploiting the benefits of shared information on the battlefield to develop a common operating picture. The DoD's aggressive pursuit of information technologies to enable network-centric warfare (NCW) will generate a significant warfighting advantage as well as potential pitfalls. The Global Information Grid (GIG) is the telecommunications infrastructure -- the network backbone -- by which the United States facilitates NCW and executes its dominant forms of strategic power, both economically and militarily. A significant portion of the GIG relies upon space-based assets and technologies that expose the United States to vulnerabilities -- the very same space-based technologies that enable NCW. This paper addresses threats to the GIG, vulnerabilities of our space-based assets, and examines concerns about the implicit reliance upon space-based technologies to execute NCW. It evaluates the strengths and weaknesses of employing space technology in a network-centric environment, considers future threats posed by adversaries using asymmetric warfare, and examines the impacts on warfighting capabilities and national security. Finally, this paper identifies and recommends measures that mitigate risk to the United States' principal enabler of NCW -- space-based technology.

ACCESSION NUMBER: ADA469763

http://handle.dtic.mil/100.2/ADA469763

Glenn, Michelle L. ***Command and Control in the Systems Technology Battle Lab***. Monterey, CA: Naval Postgraduate School, June 1999. 109p.

Abstract: Joint Vision 2010 introduces the emerging operational concepts of Dominant Maneuver. Precision Engagement, Focused Logistics, and Full Dimensional Protection enabled by Information Superiority. Information Superiority is gained through operational architectures that closely couple the capabilities of sensors, C2, and shooters. This architecture of future warfare can be characterized as Network Centric Warfare. The Navy's response to adapt and develop new operational concepts in support of Network Centric Warfare is Information Technology for the Twenty First Century (IT-21). IT-21 is a reprioritization of existing Command, Control, Communications, Computers, and Intelligence (C4I) programs of record focused on accelerating the transition to a personal computer (PC) based tactical and support warfighting network. Battle Labs exist Service wide to aid in this growth process. Battle labs are focused organizations created to explore new technology, concepts, doctrine, or tactics, techniques and procedures to improve the efficiency and combat power of the forces. The Systems Technology Battle Lab was established to inject an academic viewpoint into experiments and research sponsored by the MBC and Commander, Third Fleet (COMTHIRDFLT). Currently, the documentation on the systems installed and how they work together to provide a centralized forum for experimentation and research is inadequate. The purpose of this thesis is to provide the STBL user with a guide describing the capabilities of the STBL and an example of its utilization in an integrated form.

ACCESSION NUMBER: ADA366299

http://handle.dtic.mil/100.2/ADA366299

Gomez, Richard M. ***Centralized Command - Decentralized Execution: Implications of Operating in a Network Centric Warfare Environment***. Maxwell AFB, AL: Air University, 2003. 39p.

Abstract: Advances in technology have brought about many chances to the employment of force. Information Operations and Network Centric Warfare significantly enhance situational awareness throughout the command hierarchy and provide an avenue for the highest levels to view battlefield actions as they develop. These chances have a great impact on the leadership of military forces. The line between Centralized Command and Decentralized Execution has at times become blurred, and there is grave potential for leaders to attempt to execute the battles at the major command levels. A thorough understanding of command relationships and leadership principles at the strategic, operational, and tactical levels of conflict, coupled with increased education on the benefits and dangers of technology and information systems are required to maintain effective force employment and achieve the asymmetric effects that Network Centric Warfare can create.

ACCESSION NUMBER: ADA424 605

http://handle.dtic.mil/100.2/ADA424605

Gonzales, Daniel, et al. ***Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16***. Santa Monica, CA: Rand Corporation, 2005 136p.

Abstract: In the mid-1990s, the U.S. Air Force at the request of Congress conducted the Joint Tactical Information Distribution System (JTIDS) Operational Special Project. In this exercise, the capabilities of F-15 air superiority aircraft equipped with voice-only communications were compared with F-15s equipped with voice and JTIDS Link 16 data link communications in tactical air-to-air combat. More than 12,000 sorties were flown in this special project. Blue offensive counterair packages composed of these F-15s ranged in size from two to eight aircraft. In all cases, the packages were controlled and cued by Airborne Warning and Control System (AWACS) aircraft. The size of the engagements ranged from two Blue fighters on two Red fighters to eight Blue fighters on 16 Red fighters. Engagements occurred during daylight and night conditions. The primary independent variable was whether the Blue F-15s were equipped with the Link 16 data link or with conventional voice communications only. The capability of the Red aircraft remained consistent during the project. On average, Blue offensive counterair packages

equipped with Link 16 achieved a two-and-a-half times improvement in kill ratio (Red aircraft to Blue aircraft destroyed), both during the day and at night. However, it was unclear how and why this significant improvement in force effectiveness arose. The aim of this study is to understand whether this increase in combat effectiveness stemmed from the network-centric capabilities of F-15 aircraft equipped with Link 16 and fighter pilots able to effectively use data link communications.

ACCESSION NUMBER:ADA437368

http://handle.dtic.mil/100.2/ADA437368

Greenwood, Michael D. ***E Pluribus Unum: Enhancing Intelligence Support in the Network Centric Environment***. Newport, RI: Naval War College, February 1999. 23p.

Abstract: Network Centric Warfare's emphasis on timeliness and targeting challenges the Intelligence Community to concurrently support tactical combat operations and operational planning and execution while maintaining strategic situational awareness. To successfully accomplish each requirement obligates the Intelligence Community to make fundamental changes in the authority of the Supported Theater Intelligence Officer relative to the other members of the Intelligence Community. Additionally, a renewed emphasis must be placed on the collection of human intelligence, the development of regional expertise, and utilization of imagery analysts. Lastly, the Network Centric Warfare's requirement to concurrently support the Strategic, Operational, and Tactical levels places a premium on accessing archived intelligence via the Information Grid. As a consequence, the Intelligence Community must use available technology to filter information and better allocate analytical resources to achieve real time intelligence support.

ACCESSION NUMBER: ADA363102

http://handle.dtic.mil/100.2/ADA363102

Guthrie, Joseph W., et al. ***The Effects of Collaborative Technologies on Individual and Team Performance in a Network Centric Warfare (NCW) Environment.*** Orlando, FL: University of Central Florida, 2007. 50p.

Abstract: Organizations believe that teams are the answer to many of their problems and are implementing them more readily into their daily business practices. The ubiquitous nature of teams in organizations and the current organizational trend of focusing on a more global marketplace have changed the ways in which teams collaborate. In the public and private business sector, organizations foster global partnerships that require employees from different parts of the world to work together to develop new ideas, solve problems, and make decisions. In order to ensure that these teams continue to perform at a high level and produce desired outcomes, researchers must better understand how teams operate in collaborative environments.

ACCESSION NUMBER: ADA470167

http://handle.dtic.mil/100.2/ADA470167

Haas, Michael W., Matthew S. Middenorf, and Shari Ulring. ***The SAFIRE and an Initial Network-Centric Warfare Evaluation***. Wright-Patterson AFB, OH: Air Force Research Laboratory, 2006. 59p.

Abstract: Two major purposes are served by this report. The first is to describe the Synthesized and Human Aerospace Forces in an immersive Research Environment (SAFIRE), a simulation capability linking many of the Warfighter Interface Division's (AFRL/HEC) human-in-the-loop simulations together as well as with external AFRL and AFMC assets. The second purpose is to document the initial use of the SAFIRE architecture in its intended role, as a tool supporting evaluations of crew-system interfaces used in a network-centric environment. Information availability was manipulated experimentally during simulated air-to-air combat simulations of an air base defense mission scenario that involved multiple friendly and adversary aircraft as well as simulated airborne command and control. Statistical analysis of resultant data indicated that the manipulation of information availability did affect both objective measures of performance and subjective measures of situation awareness. The presence of these effects clearly demonstrates SAFIRE's ability to support crew-system interface evaluations. In addition, the presence of

a practice effect was observed indicating more attention should be focused on experimental design issues for future studies to reduce this effect or to compensate for its presence.
ACCESSION NUMBER: ADA457041
http://handle.dtic.mil/100.2/ADA457041

Hakimzadeh, Kavon. ***The Issue of Decision Up-Creep in Network Centric Warfare***. Newport, RI: Naval War College, 2003. 24p.
Abstract: Network Centric Warfare (NCW) will provide operational commanders with unprecedented access to tactical level information. Depending on any number of external factors from politics to personality, access to this information may tempt operational commanders to micromanage the tactical actions of their subordinates. While it is the commander's prerogative to make decisions for any level of the force, the problem of "decision up-creep" could undermine synchronization on the tactical level and undo many of the war fighting benefits derived from a fully netted force. This paper serves three purposes. First, through the use of examples from recent operations, it shows that the unprecedented "reach" provided by NCW will increase the operational commander's temptation to micromanage tactical actions. Second this paper shows that decision up-creep would virtually negate all of the benefits of NCW. Finally, this paper presents organizational, doctrinal and cultural alternatives for mitigating decision up-creep.
ACCESSION NUMBER: 415482
http://handle.dtic.mil/100.2/ADA415482

Hannon, Jeffery A. ***Network Centric Warfare and Its Effect on Unit of Employmentx (UEx) Use of Mission Command***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2005, 57p.
Abstract: The 2002 NSS call for "transforming to meet the challenges and opportunities of the twenty-first century", and the Army's leadership elected to concentrate the service's transformation efforts on battle command. The three pillars supporting the U.S. Army's transformation of battle command are its doctrine of mission command, reorganization of its warfighting forces - including the creation of the Unit of Employment (x) (UEx) headquarters - and the emerging joint concept of network centric warfare (NCW). The decision to merge these practices and concepts, coupled with the focus on transformation through battle command, necessitates understanding how network centric warfare may affect the UEX's use of mission command doctrine. FM 6-0, Mission Command: Command and Control of Army Forces, states that trust and mutual understanding underpin the practice of mission command. Evaluated against these two principles, the Army's move to a brigade-based force, coupled with policy changes and emerging warfighting concepts, improves UE(x) commanders' ability to exercise mission command. These improvements overshadow the tendency of commanders to diminish trust and mutual understanding by relying on centralized command and control practices, which result from the influence of U.S. Army policies, UE (x)structural and conceptual limitations, and features of network centric warfare theory.
ACCESSION NUMBER: ADA435895
http://handle.dtic.mil/100.2/ADA435895

Hansen, Donald K. ***Can Decentralized Command and Control Complement Network-Centric Warfare?*** Newport, RI: Naval War College, 2004. 21p.
Abstract: Future technology will allow the Joint Force Commander unprecedented access to the tactical level of war. Depending on his personality, he may chose to directly control events unfolding at the tactical level or leave the fighting to individuals charged with employing their weapon systems. The ability of a pilot, tank driver or infantry battalion commander in the future to share his operational picture with the entire chain of command (shared situational awareness) and vice versa, begs the need for sound, authoritative command and control doctrine to maximize the inherent benefits of this information advantage. All players in this future system must share a common rule set in order to exploit the war fighting advantages described in Joint Vision 2020 (JV 2020). Command and control doctrine must now outline this new rule set. With a common rule set, reorganization, training and education of staffs and

combat units can begin. Overcoming old paradigms will be difficult, but by applying the doctrine of maneuver warfare to Network-centric Warfare (NCW) and JV 2020 concepts, a better command and control method can be implemented. The purpose of this paper is to reconcile the conflicts between maneuver warfare doctrine and the warfighting concepts currently being developed under JV 2020 and NCW by establishing a strong case for decentralized command and control.

ACCESSION NUMBER: ADA422815

http://handle.dtic.mil/100.2/ADA422815

Harvey, Charles and Lance Schultz. ***Analysis of the Impact of Network-Centric Warfare on the Doctrine and Tactics, Techniques and Procedures of Intelligence at the Operational Level***. Newport, RI: Naval War College, June 1999. 69p.

Abstract: *This project sought to determine the impacts of network centric warfare (NCW) on the planning and direction of intelligence at the operational level, and what changes in joint intelligence doctrine (JID) and tactics, techniques, and procedures (TTPs) should/should not be made to support it? To meet those objectives, the analysis compared the NCW concept to the fundamentals upon which intelligence is to be employed in military operations (intelligence doctrine), the plans for taking doctrine to the field (the TTPs), and how the TTPs become reality in a real world operation (DESERT FOX). To serve as a point of departure, a working model for Now was established from the current literature. (This paper has classified appendices)*

ACCESSION NUMBER: ADA370496

http://handle.dtic.mil/100.2/ADA370496

Heaney, Thomas A., Jr. ***Battle Command and Network-Centric Warfare: Putting First Things First.*** Newport, RI: Naval War College, 2001. 28p.

Abstract: *At the dawn of the information Age, the commander's concept of operation, for arranging potential combat power into victorious campaigns, major operations, and battles, is still the essence of military operations. It is the commander who translates higher concepts and guidance, from the strategic to tactical levels of war, through his visualization of the operation to accomplish the mission Consequently, his concept of operation directs all battlefield activities to achieve the desired military end-state. Network-Centric Warfare is a technologically based process designed to harness the power of the Information Age by exploiting technological advances to achieve dominance in the information domain. Through a network of new systems (sensors, information, and weapons), warfighters translate this information into dominant warfare-centered Network-Centric Operations (NCO). NCO shifts the operational paradigm from platform-centric to effects-based operations, by linking geographically dispersed warfighters (through a common operational picture) to overwhelm potential adversaries.*

ACCESSION NUMBER: ADA393569

http://handle.dtic.mil/100.2/ADA393569

Heickero, Roland. ***Some Thoughts on the Application of Military Theory to Information Operations and Network Centric Warfare.*** Stockholm, Sweden: Swedish Defence Research Agency, 2006. 27p.

Abstract: *The transformation into a world based on communication and information leads to Information Operations (IO) becoming more important than ever. Thus, there is a need to develop new methodologies for successful IO that take into account the change towards network-enabling warfare capabilities. In a network-centric warfare approach it is important to understand the opponents' network structure and communication system and how they use these resources. Equally important is to understand one's own network structure in terms of strengths and weaknesses. Every type of network has it own vulnerabilities in the form of vital nodes, links, and platforms, regardless of whether it is a communications, organizational, or biological network. If one understand one's own structure as well as that of one's opponents, the chances of effective IO increase greatly. A fruitful way forward is to use theories based on center of gravity (CoG) and critical vulnerabilities (CV). This paper first discusses the logic of networks in general terms and then considers different types of networks and their respective abilities to resist attacks*

of different kinds due to center of gravity and critical vulnerabilities. Twenty briefing charts summarize the presentation.

ACCESSION NUMBER: ADA461536

http://handle.dtic.mil/100.2/ADA461536

Helme, E. C., III. ***Diminishing the Critical Vulnerability of Space***. Newport, RI: Naval War College, Joint Military Operations Department, February 1998. 21p.

Abstract: Network-centric warfare (NCW) relies heavily on the exploitation of space and technology to create a more efficient, effective end responsive form of combat power than is presently available to United States forces. The backbone of NCW is the advanced communication and sensor systems that reside in space. These data paths produce a flow of information that promises a greater military reach, irrespective of force size, and supports an increasing trend toward power projection in an ERA of diminishing forward bases. Unfortunately, our propensity to levy an increasing number of systems upon the skeleton of space has increased its importance as a target to any potential future adversary. Furthermore, a shift to NCW would mark a potentially dangerous commitment to electronic connectivity in order to assure combat power. This increased risk results from the fragility of space assets because components of our space architecture are assailable with relatively low cost, low technology weapons and tactics. Therefore, if we recognize these assets as a critical vulnerability, bow do we reconcile a trend toward increasing our dependence on space. The solution requires an environment of innovation that strives to balance hardware, techniques and skills in such a way that realizes the advantages of network-centric warfare without compromising the combat power of individual platforms. Preserving the capability of platform-centric warfare reduces the vulnerability of space assets and safeguards our ability to mass effects regardless of connectivity.

ACCESSION NUMBER: ADA349256

http://handle.dtic.mil/100.2/ADA349256

Henseler, Sean P. ***Addressing the Legal Challenges of Network Centric Warfare. Case In Point: The Legal Implications of Obtaining an "Information and Knowledge Advantage" Prior to Hostilities.*** Newport, RI: Naval War College, 2001. 28p.

Abstract: If it is true that the Navy is moving away from platform-centric toward network-centric warfare (NCW), then its leaders must ensure that any such transition is accomplished in the most efficient and effective manner possible. Since the Navy's current vision of net-centric operations raises many complex and often unsettled legal issues, the Navy must establish a formal framework for analyzing the legal challenges posed by NCW then integrate this framework into any NCW transition process. Future net-centric operational commanders have a vested interest in ensuring that the legal implications of NCW on factor space, time, and forces have been thoroughly considered. Current and future international and domestic law might limit the ability of net-centric commanders to optimize the key concepts of the Navy's vision of net-centric operations. If the technological and doctrinal aspects of NCW continue to rapidly evolve without regard for the legal challenges, the Navy might find itself in a position where it has invested a tremendous amount of time and money developing a system of sensors and platforms that cannot be employed as envisioned due to legal constraints.

ACCESSION NUMBER: ADA389546

http://handle.dtic.mil/100.2/ADA389546

Hestad, Daniel R. ***A Discretionary-Mandatory Model as Applied to Network Centric Warfare and Information Operations.*** Monterey, CA: Naval Postgraduate School, 2001. 97p.

Abstract: The concepts of DoD information operations and network centric warfare are still in their infancy. In order to develop concepts, the right conceptual models need to be developed from which to design and implement these concepts. Information operations and network centric warfare are fundamentally based on trust decisions. However, the key to developing these concepts is for DoD to

develop the organizational framework from which trust, inside and outside, of an organization may be achieved and used to its advantage. In this thesis, an organizational model is submitted for review to be applied to DoD information systems and operational organizations.

ACCESSION NUMBER: ADA387764

http://handle.dtic.mil/100.2/ADA387764

http://bosun.nps.edu/uhtbin/hyperion-image.exe/01Mar_Hestad.pdf

Hilton, Paul K. ***Expeditionary Maneuver: A Synthesis of Network Centric Concepts***. Newport, RI: Naval War College, 2003. 21p.

Abstract: Expeditionary Maneuver Warfare (EMW) is a unique and appropriate concept for 21st century warfare because it is a synthesis of the best of traditional realistic warfare concepts, stable maneuver warfare doctrine, and the contemporary concepts of network centric warfare (NCW). The Marine Corps EMW concept emphasizes the realities of confusion, human factors, danger, and uncertainty to craft a concept that relies on well-trained and motivated people. The NCW concept is about how the network will provide synergy and added combat power by accomplishing tasks that formerly required standing forces. EMW is about tailored forces to accomplish a mission and using maneuver to get there. NCW is about the network helping to share resources to get the right combat capability to the right place and time. EMW on the battlefield today will rely heavily on a robust and ubiquitous network, but it will not be entirely dependent on the network. The author concludes that the two concepts are compatible articulations of modern warfare.

ACCESSION NUMBER: ADA420212

http://handle.dtic.mil/100.2/ADA420212

Honabarger, Jason B. ***Modeling Network Centric Warfare (NCW) With the System Effectiveness Analysis Simulation (SEAS).*** Wright-Patterson AFB, OH: Air Force Institute of Technology, 2006. 108p.

Abstract: Significant technological advances over the past few decades have fueled the continual and rapid development of an information-based world. Network Centric Warfare (NCW) has become the buzzword of the young millennium within the Department of Defense (DoD) and is quickly becoming a popularly shared vision and rallying cry for force transformation among United States military leaders. An essential element in fully implementing this network-centric way of thinking is to develop useful measures to help gauge the effectiveness and efficiency of both our military networks and our strategic NCW doctrine. The goal of this research is first to provide a comprehensive summary of the key literary works that have forged a foundational basis for defining NCW. Second, this work will utilize a System Effectiveness Analysis Simulation (SEAS) combat model, which represents a Kosovo-like engagement (provided by the Space and Missile Center), to serve as a tool in exploring the use of NCW metrics in military worth analysis. Third and last, this effort selects measures for the physical, information, and cognitive domains of NCW and analyzes the outputs from the Kosovo scenario that are pertinent to each domain in order to assess the usefulness of each metric. In the final analysis, the average target detection distance outputs and average communication channel message loading metrics chosen for the physical and information domains yielded mixed results and levels of utility.

ACCESSION NUMBER: ADA446395

http://handle.dtic.mil/100.2/ADA446395

Hooper, Gary R. ***Command Concepts and Staff Organization for Joint Vision 2010***. Newport, RI: Naval War College, February 1998. 27p.

Abstract: Joint Vision 2010 (JV 2010) describes the need for new procedures and organizations to implement its concepts. Two significant and inseparable issues are how forces will be commanded and how the Joint Force Commander will organize his staff to conduct the type of operations described in JY 2010. JV 2010 places a premium on Information Age concepts such as non-linear dynamics, speed of command, network-centric warfare, and blurred levels of war. Our present hierarchical command structure, which is based upon linear reductionism, is inappropriate for Information Age operations.

Additionally, the doctrine of 'centralized planning, decentralized execution' is not flexible enough to handle the full spectrum of envisioned military operations. A more flexible command concept is required. A 'Flat Ring' model for staff functions which emphasizes speed of command and network operations is described and recommended.
ACCESSION NUMBER: ADA348415
http://handle.dtic.mil/100.2/ADA348415

Huffaker, Jacob A. **The Benefit of 802.20 Technologies on Information Flow in Network Centric Warfare.** Monterey, CA: Naval Postgraduate School, 2005 57p.
Abstract: *This thesis will focus on the area of 802.20 wireless networking and how this technology will vastly benefit the US military forces, especially in the Network Centric concept of operations, where information flow is crucial. It will investigate this technology using published literature and previously gathered experimental data. This thesis will then relate its findings to Network Centric Warfare and the matters that could be most affected by this new technology.*
ACCESSION NUMBER: ADA439218
http://handle.dtic.mil/100.2/ADA439218
http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Sep%5FHuffaker.pdf

A Human-Centric Architecture for Net-Centric Operations. Vienna, VA: Evidence Based Research, 2005. 64p.
Abstract: *Net-Centric Operations seek to improve military effectiveness among spatially distributed and possibly culturally diverse teams. Key to the net-centric operational concept are agile teams that excel even in the most difficult circumstances. Such teams can self-synchronize, smoothly coordinating to exploit the diverse perspectives and expertise within the team. The members of such teams are on the same wavelength, continually making adjustments to leverage each others abilities and to accommodate each others needs. Recent research on the cognitive foundations of collaboration and teamwork has identified key cognitive enablers to effective teamwork. These cognitive enablers are the knowledge and understandings that team members require to work together successfully. Accordingly, it is very desirable that teams acquire and maintain this knowledge. There are three technical prerequisites to ensure that spatially distributed team members can do this: an architecture that provides reliable communications connectivity among team members; information that supports task performance and team coordination; and a means for team members to evaluate performance and correct problems. This report describes how to create an infrastructure that achieves these technical prerequisites.*
ACCESSION NUMBER: ADA430546
http://handle.dtic.mil/100.2/ADA430546

Kearney, Kevin N. ***Denial and Deception--Network-Centric Challenge***. Newport, RI: Naval War College, February 1999. 24p.
Abstract: *Adversarial denial and deception (D&D) poses a serious challenge to future operational concepts based on perceived informational superiority. An analysis of how D&D may interact in a future network centric environment demonstrates some inherent vulnerabilities of information technology (IT) based warfighting theory. Operational D&D has continued to keep pace with sensor development and through physical, technical and administrative means will be able to influence sensor derived information. Once our information is tainted, network centric's reliance on information dominance will become a vulnerability. Deception will travel at high speeds and effect multiple operational levels due to the networked operational picture provided by network centric theory. Our dependence on reliable and timely information, if affected by D&D, may lead to ambiguity, misdirection, and/or false security. Network centric's speed of command will further exasperate D&D's effect by increasing the speed of deception while simultaneously reducing the likely identification of deception through analysis. Our speed and networked precision may also finely hone our operational art to the point of making us predictable and therefore more susceptible to adversarial D&D. The additional network centric attributes of self synchronization, platform reduction, and adversarial lock out will also contribute to our vulnerability to*

D&D by creating an environment of enemy underestimation and increasing the severity of consequences of friendly action taken under the influence of adversarial D&D. The D&D challenge that network centric warfighting faces can be addressed through an increased emphasis on the importance of networked analysis. Additionally, future doctrine must reflect a clear understanding of anti-D&D methodologies so that operational commanders of the future are aware of and can plan how to counter D&D when they face it.

ACCESSION NUMBER: ADA363099

http://handle.dtic.mil/100.2/ADA363099

Klingbeil, Ralph S. and Keith M. Sullivan. ***A Proposed Framework for Network-Centric Maritime Warfare Analysis***. Newport, RI: Naval Undersea Warfare Center, 2003. 16p.

Abstract: The benefits of network-centric warfare are addressed in many publications, but few of these publications actually demonstrate how to quantify these alleged benefits. This report proposes an analytical framework to quantify the value-added of network-centric warfare; that framework is queueing theory, which is based on the concept of a demand-for-service process. Most warfare tasks can be characterized as demand-for-service processes. This report shows how queueing theory can be applied to demand-for-service warfare tasks and thus provide the basis for analyzing and quantifying those tasks. In addition, this report demonstrates how the functions of many of the independent and dependent variables and associated warfare metrics can be translated into the characteristics and metrics of queues.

ACCESSION NUMBER: ADA416829

http://handle.dtic.mil/100.2/ADA416829

Knight, Michele, Les Vencel and Terry Moon. ***A Network Centric Warfare (NCW) Compliance Process for Australian Defence***. Edinburgh, Australia: Defence Science and Technology Organisation, 2006. 85p.

Abstract: The NCW Program Office (NCWPO) is responsible for ensuring that the ADF's capability projects are Network Centric Warfare (NCW) compliant, from the time they are listed in the Defence Capability Plan until they enter service as realised capabilities and throughout life-of-type. The NCWPO has engaged a number of different groups to look at the problem of NCW Compliance from different perspectives. This report describes one of these studies. It proposes an NCW Compliance Process that is based on a simple underlying conceptual model. It also identifies some critical issues to be addressed by the NCWPO in order to improve the rigour and quality of the NCW Compliance Process.

ACCESSION NUMBER: ADA462949

http://handle.dtic.mil/100.2/ADA462949

Kuhn, James K. ***Network Centric Warfare: The End of Objective Oriented Command and Control***. Newport, RI: Naval War College, February 1998. 28p.

Abstract: The rapid incorporation of emerging technologies, particularly information technologies, in the military presents both tremendous opportunities and challenges for all aspects of the American way of war. One of the most significant impacts of information technology on the military is being called a new form of warfare: network-centric. Network-centric warfare is the enabling concept for JV2010 and Concept for Future Joint Operations. It proposes to revolutionize war through the emerging concepts of speed of command and self-synchronization. A totally new approach to warfare, it is characterized by unique strengths and weaknesses. Most significant of these is its impact on command and control of forces throughout the battlespace. The current US command and control system is based on an objective-oriented approach to command. However, it does not create the conditions for the quantum improvements in effective employment of assets foreseen by network-centric warfare. Network-centric warfare, then, requires a different command and control system to realize the full potential of JV2010.

ACCESSION NUMBER: ADA348447

http://handle.dtic.mil/100.2/ADA348447

Lim, Soon-Chia. ***Network Centric Warfare: A Command and Control Perspective***. Monterey, CA: Naval Postgraduate School, 2004. 105p.

Abstract: This paper seeks to analyze the command and control issues an sing from the advent of NCW. While information superiority is not a new concept, the blazing speed of advancement in information technologies have brought about dramatic changes to other lifestyles and profound changes in the conduct of modern warfare. This leads to the birth of Network Centric Warfare. NCW offers great opportunities to dramatically enhance combat prowess by establishing shared situational awareness, increasing speed of command, improving systems' lethality and survivability, and enabling greater flexibility through self synchronization. However, these revolutionary changes in NCW do not depend on technology alone. In order to harness the full benefits of NCW, the full span of elements ranging from organization, doctrine operational concepts to training must co-evolve.

ACCESSION NUMBER: ADA422430

http://handle.dtic.mil/100.2/ADA422430

http://bosun.nps.edu/uhtbin/hyperion-image.exe/04Mar%5FLim%5FS.pdf

Livingood, Debra M. ***The Integration of Civil Relief Agencies Into Network Centric Warfare***. Newport, RI: Naval War College, 2002. 26p.

Abstract: The U.S. military is currently in the process of undergoing a visionary transformation of its forces using technological advances with the goal of maintaining global superiority into and beyond the 21st century. The single most important technological advancement that will transform the military and allow it to attain full spectrum dominance will be the capability to effectively capture and integrate the vast amount of information on individual networks into a Common Operating Picture (COP). The military's vision is to accomplish this with Network Centric Warfare (NCW) through the integration of informational grids. The military, though, continues to maintain its focus narrowly on information obtained by military sources only and is neglecting to include another significant information source: civil relief agencies. In order to achieve true information superiority the information from thousands of civil relief agencies needs to be integrated into the COP. Over the past decade the U.S. military has been heavily involved with Military Operations Other Than War (MOOTW) which, by its nature, includes interaction with numerous civil relief agencies. Throughout all of these operations, the critical importance of efficiently sharing information between the military and these agencies has been proven over and over again. This is especially true in MOOTW, but as Operation Enduring Freedom has shown, it is also important in war. Therefore, to neglect developing methods to integrate the civil relief agencies' vital information into the COP could prove to be disastrous.

ACCESSION NUMBER: ADA405613

http://handle.dtic.mil/100.2/ADA405613

Llinas, James. ***Service-Oriented Architectures, Network-Centric Warfare, and Agile, Self-Synchronized C2: Impacts to Data Fusion Process Design.*** Buffalo, NY: State University of New York - Buffalo, 2006. 79p.

Abstract: One of the primary if not the central motivating rationale for Network-Centric Warfare (NCW) is that NCW provides an enabling mechanism for information sharing and shared understanding and awareness of military situations of interest, that in turn allows the realization of entirely new concepts of C2 that are advertised as providing greatly increased agility, speed of command, and synchronization in C2. In turn, the underlying enabling IT mechanism for NCW is the Service-Oriented Architecture (SOA) concept, within which all functional services, to include Data Fusion Services, will presumably operate. These attractive but as-yet-not-fully-defined concepts represent a challenge to the Data Fusion community in terms of understanding the implications of the evolving NCW, SOA, and new C2 concepts on the design of Data Fusion Services. Key to this understanding in particular is the need for a close dialog with the C2 research community on exactly what the information needs of new C2 concepts will be and how those needs can best be met by appropriately-designed Data Fusion Services. This talk will address each of these issues and argue for the need for both: (1) a multi-community approach to the

architecting of effective and efficient SOA's, and (2) for new initiatives in distributed Data Fusion to address the specific technical challenges of NCW-specific Data Fusion Service design and implementation. (It should be noted that this paper is drawn largely from US literature and so presents a US-based viewpoint developed by the author; the paper does not represent any official US governmental views.) This brief paper is intended to sketch the topical areas that will be addressed in the associated Keynote speech.

ACCESSION NUMBER: ADA474190

http://handle.dtic.mil/100.2/ADA474190

Logan, Charles J. ***Complexity at the Battle of Midway: Implications for Network-Centric Warfare***. Newport, RI: Naval War College, 2001. 23p.

Abstract: The lessons of the battle of Midway are relevant to the U.S. Navy's effort to implement network-centric warfare. Japanese forces at the battle were superior to those of the United States both in number and quality. Both forces employed the same technology and similar tactics. The margin of U.S. victory was superior intelligence, and command and control that relied on the initiative of subordinates to self-organize to defeat the enemy. U.S. execution of the Midway battle plan exemplified the tenets of shared awareness, speed of command, and self-synchronization to meet the commander's intent that will underpin the network-centric Navy. The U.S. Navy must adapt its concept of command and control to realize fully the benefits of network-centric operations. Navy doctrine should more explicitly recognize that its fighting forces are a complex adaptive system and command them as such. Control should become less rather than more centralized as the result of more information. The commander's intent will become even more important as subordinate levels of command gain more information and power to influence the battle. The principles of war, particularly simplicity, will retain their importance in the network-centric environment.

ACCESSION NUMBER: ADA393506

http://handle.dtic.mil/100.2/ADA393506

Maguire, Gregory M. ***Concept of a Dynamic Organizational Schema for a Network-Centric Organization***. Monterey, CA: Naval Postgraduate School, 2003. 119p.

Abstract: Organizational structure has profound effects on a joint force commander's ability to perform military actions. Organizations and their environment exhibit an interdependent relationship, requiring a commander to evolve his organization to rapidly achieve mission accomplishment. The CNO Strategic Studies Group XIX report of September 2000 has identified the FORCEnet as being the basis for the U.S. Navy's future network-centric organization, and outlines a military environment that includes multitudes of manned and unmanned vehicles, platforms, sensors, weapons and warfighters. These naval elements will operate jointly, leveraging organizational structure to rapidly sense, assess, and respond to the defense of the nation's security interests as directed by the President. The focus of this research is to examine this envisioned future military environment, the military actions required to achieve success in that environment and the organizational structure(s) that will best fit those action requirements.

ACCESSION NUMBER: ADA417518

http://handle.dtic.mil/100.2/ADA417518

McCarthy, Shannon E. ***Marketing Network Centric Warfare***. Newport, RI: Naval War College, 2001. 23p.

Abstract: The Navy has created an innovative concept to fight future wars and deal with operations other than war-network centric warfare (NCW) . Unfortunately, NCW remains a Navy premise that is not well recognized or accepted by its own members or those of the other services. In order to be effective, NCW must transition from a Navy concept to a joint product. NCW advocates can effect this transition by using basic business principles to market NCW. They can tailor a solid mix of product, price, place, and promotion to target and win over operational commanders. This is the first and vital step to successfully introduce NCW as the way of the future.

ACCESSION NUMBER: ADA389557

http://handle.dtic.mil/100.2/ADA389557

Monroe, Deborah. ***Net-Centric Warfare: Are We Ready to be Cyber-Warriors?*** Newport, RI: Naval War College, May 1999. 21p.

Abstract: Joint Vision 2010, the Chairman of the Joint Chiefs of Staff's template for future military operations, identifies information superiority as the linchpin of the emerging operational concepts of Dominant Maneuver, precision Engagement, Focused Logistics and Full Dimensional protection. While the technical challenges to realizing these concepts are acknowledged, I contend the tasks required to successfully integrate the human and cultural side of Joint Vision 2010's information superiority are as daunting as any of the still unsolved technical hurdles. Currently, the human element of technology enabled warfare is not getting the attention it needs. The military must begin to examine whether current training and doctrine are sufficient to prepare operational commanders for the Chairman's vision of the future.

ACCESSION NUMBER: ADA370751

http://handle.dtic.mil/100.2/ADA370751

Morua, Michael L. ***Network Centric Operations: The Enterprise Battle Group Experience***. Annapolis, MD: Naval Academy, 2002. 11p.

Abstract: With increased information flow and rapidly paced military operations, decision makers find it difficult to maintain full situational awareness, resulting in ineffective decision-making in stressful and time-constrained environments. How does one manage increased information loads in a shorter time without negatively impacting decision-makers? Due to the competitive nature of warfare and a commander's desire to gain a military advantage over an enemy, military operations can become fast paced. in terms of Boyd's OODA (Observe, Orient, Decide Act) Loop, when a dynamic OODA Loop process is combined with real-time, high volume, networked information systems currently accessible on ships, the naval decision maker/operator can now better respond to the action and seize the initiative in battle. The Information Technology (IT) revolution has made sailors accessible to e-mail, electronic documents, Internet web-pages, chatrooms, and video teleconferencing. However, unconstrained/uncontrolled use of information resources can quickly overwhelm operators and cause information overload. The Navy's doctrine on Network Centric Operations exploits the advances in IT-21 systems in order to improve the OODA loop process, determine the enemy's vulnerabilities, and finally achieve the desired end-state. Network Centric Operations focus combative power from the network rather than individual platforms. IT and Network Centric innovations that were demonstrated during Enterprise Battle Group's (ENTBATGRU) 2002 Deployment will be discussed.

ACCESSION NUMBER: ADA400008

http://handle.dtic.mil/100.2/ADA400008

Moses, Bruce D. ***Intelligence Collection: Supporting Full Spectrum Dominance and Network Centric Warfare?*** Fort Leavenworth, KS: Army Command and General Staff College, Schools of Advanced Military Studies, 2004. 82p.

Abstract: This monograph examines whether the Army's information collection efforts are supporting the goal of full spectrum dominance and whether these are in harmony with the concepts of network centric warfare. Full spectrum dominance and network centric warfare are central themes in Department of Defense and Army transformation literature and both require information collection and an understanding of the role of cognition empowered by networking for success. More specifically, it examines whether Army collection efforts are focusing too heavily on collection for combat operations and leaving it unable to fully exploit the access to adversary systems during stability operations. This study found that the institutional Army is not fully supporting the goal of full spectrum dominance or network centric warfare but is still myopically investing heavily in efforts to defeat the adversary's conventional capabilities with standoff collection technology and is not creating the organizational, systems and technical architectures necessary to leverage the power of a fully networked force.

ACCESSION NUMBER: ADA432929

http://handle.dtic.mil/100.2/ADA432929

Mosley, Robbie L. ***Network Centric Warfare: Does Funding Priorities Support the Strategy?*** Carlisle Barracks, PA: Army War College, 2006. 22p.

Abstract: Network Centric Warfare is a central component of the Defense Department's transformation initiatives. It continues the journey of transforming the military services into joint capabilities-based formations for meeting the challenges of the 21st Century. The following analysis provides a microscopic slice of the Defense Department's transformational concepts for the military. The Army's Future Combat System serves as an excellent case study for reviewing some key elements of defense transformation and the feasibility of funding network centric operations. This paper examines issues with the processes for obtaining the necessary resources to include the complexities of transforming a military service. Finally the paper provides recommendations on ensuring the successful implementation of the transformation objectives. While the Military Departments are updating their operational constructs toward Network Centric Warfare Vision the funding debates reflect a significant gap in obtaining the necessary resources for full implementation. In essence Network Centric Warfare is struggling for valuable resources and may falter due to the de-synchronization of intra-dependent programs.

ACCESSION NUMBER: ADA449235

http://handle.dtic.mil/100.2/ADA449235

Neely, David S. ***Network-Centric Commander's Intent: The Key to Network-Centric.*** Newport, RI: Naval War College, 2003. 28p.

Abstract: There are many views about how the still-developing concept of Network-Centric Warfare will transform our U.S. military. Operational commanders, leading military forces at the operational level of war, will remain relevant and essential to the effective conduct of Network-Centric Warfare. The key question is how an operational commander can effectively command his dispersed and decentralized forces while taking advantage of the capabilities offered by Network-Centric Warfare. A formal statement of clear, concise Commander's Intent is currently the primary means by which operational commanders guide the effective warfighting of their subordinate commands. A revised and improved style of Commander's Intent that capitalizes on new capabilities will be essential to effective Network-Centric Warfare.

ACCESSION NUMBER: ADA420277

http://handle.dtic.mil/100.2/ADA420277

Nissen, Mark E. ***Understanding "Understanding" Flow for Network-Centric Warfare: Military Knowledge-Flow Mechanics***. Monterey, CA: Naval Postgraduate School, 2002. 50p.

Abstract: Network-centric warfare (NCW) emphasizes information superiority for battlespace efficacy, but it is clear that the mechanics of how knowledge flows are just as important as those pertaining to the networks and communication systems used to transmit data and information. Unfortunately, with the strong presumption that knowledge is distinct from data and information, knowledge-flow mechanics in the warfare context are not well understood; even the term knowledge is used in conflicting ways (e.g., to describe information flows) by NCW experts, operational personnel and developers of military doctrine. Mapping key concepts from technologically enabled business models in which NCW is based in large part to the military, we substitute the term understanding flow when discussing the mechanics of how knowledge flows in the NCW context. In one respect, this mapping and terminological substitution enable us to move forward and model knowledge-flow mechanics in a manner that is consistent with the operational Navy's lexicon; in another respect, however, it is clear that Navy lexicon does not yet include the term understanding flow. Hence, naval conceptualization of NCW may be missing a vital element. Informed by recent advances in knowledge-flow theory, the research described in this technical report develops a four-dimensional model of understanding-flow mechanics. This multidimensional model enables a novel capability to recognize a variety of understanding-flow patterns found in the military enterprise, to distinguish such patterns from their counterparts pertaining to information and data, and to

enhance the speed and efficiency of NCW understanding flows. Just as understanding the mechanics of electrical flow is critical to developing useful electronic devices, understanding the mechanics of understanding flow is critical to conceiving useful NCW systems.

ACCESSION NUMBER: ADA406729

http://handle.dtic.mil/100.2/ADA406729

Olmo, Frank J. ***Command and Control in Joint Vision 2010: Flexible, Adaptive and Networked***. Newport, RI: Naval War College, Joint Military Operations Department, February 1999. 25p.

Abstract: One of the most daunting tasks the U.S. military will face in the 21st century is the issue of implementing effective command and control (C2) of joint and coalition military operations. As new technologies are implemented to support Joint Vision 2010 (JV2010), successful C2 must give the commander the flexibility to use faster and more accurate information technologies in order to increase battlespace knowledge and situational awareness. The dynamics of new technologies is linked to the Information Age and is commonly referred to as a Revolution in Military Affairs (RMA), which is leveraged through the enabling concepts of 'Information Superiority' and 'Network-Centric Warfare'. The challenge for the future commander is to exploit the RMA by applying a flexible C2 process to control the battlespace. Thus, as networked forces bring faster and more accurate information across all levels of war, the operational commander will exert his influence by maintaining a flexible networked architecture through a continuum based on his intent and the tempo of operations. A more focused understanding of networked C2 is the key to the evolution of new and existing joint architectures in order to keep pace with information technologies. The military must embrace an aggressive transition to a more flexible organization that is linked to a networked hierarchy to meet the challenges of the 21st Century.

ACCESSION NUMBER: ADA363260

http://handle.dtic.mil/100.2/ADA363260

Olsson, Eric J. ***Literature Survey on Network Concepts and Measures to Support Research in Network-Centric.*** Monterey, CA: Naval Postgraduate School, 2003. 89p.

Abstract: The United States Navy and its joint partners continually seek to maintain a responsive, agile, and effective fighting force well suited to combat present-day threats to national security. As a result, U.S. forces are currently undergoing force transformation to adopt an organizational structure capable of supporting this mission. This new organizational structure is known as Network-Centric Warfare. The purpose of this research is to analyze any performance metrics, measures of effectiveness, or analytical methods used by existing organizations engaged in network-centric operations that would assist the Navy and joint forces along with their transformation process. This research will be done in the form of a literature review, examining existing material written on communication, economic/business, and social/organizational networks. In addition to identifying quantitative and qualitative metrics, an emphasis will be placed on the methodologies used for network assessment. Final sections relate findings from each resource to Network-Centric Warfare and address matters relevant to the future of force transformation.

ACCESSION NUMBER: ADA417514

http://handle.dtic.mil/100.2/ADA417514

Osmun, Richard O. ***Building the Intelligence Foundation for Network Centric Warfare***. Newport, RI: Naval War College, 2001. 31p.

Abstract: The world is undergoing an information revolution with the rapid advance of information technologies. Undoubtedly, information operations is becoming more dynamic and essential to daily activities of the United States military services. Within the Department of Defense (DoD) many concepts have evolved which formulate utilizing the virtual information domain to support operations in the traditional physical domains of land, sea, air and space. One such concept, Network Centric Warfare (NCW), defines and describes how the US military should organize and fight in the information age. By

incorporating an intelligence analysis grid, the concept of NCW will optimize the utility of available information and produce shared awareness.
ACCESSION NUMBER: ADA393521
http://handle.dtic.mil/100.2/ADA393521

***Performance Learning Roadmap: A Network-Centric Approach for Engaged Learners*.** Ft. Belvoir, VA: National Defense University, 2005. 32p.
Abstract: The Acquisition, Technology and Logistics (AT&L) workplace is rapidly evolving to transform the way we conduct business. Spread all over the world to provide critical systems and support to the warfighter, our workforce demands responsive, point-of-need learning, the ability to access knowledge, and the ability to collaborate with experts at the point of-need. The Defense Acquisition University (DAU) is developing learning and job performance support systems that remain with the AT&L workforce 24 /7 and throughout their careers the concept of "continuous presence. Our focus is to shape a network-centrlc learning environment and exploit online resources and expertise. At the same time, we continue to reshape and improve our resident learning assets.
ACCESSION NUMBER: ADA436500
http://handle.dtic.mil/100.2/ADA436500

Poole, James A. ***Challenge of Netwar for the Operational Commander***. Newport, RI: Naval War College, Joint Military Operations Department, March 1996. 30p.
Abstract: The threat of intrusions to U.S. domestic and military infrastructure and information systems is very real and may affect our national security now and in the future. Information has become a new center of gravity that must be protected. Netwar is one tool of Information Warfare that the operational commander can use in defensive and offensive operations to gain information dominance. Netwar targets military or civilian non-weapons computer networks to gain a military advantage while it protects one's own systems from attack. With an overview of Netwar concepts, this paper explores the benefits of Netwar for the commander, the defensive and offensive decisions that must be made, and some prescriptions for the future that will enable the commander to fight and win conflicts effectively in the twenty-first century.
ACCESSION NUMBER: ADA307334
http://handle.dtic.mil/100.2/ADA307334

Porter, Carl D. ***Network Centric Warfare - Transforming the U.S. Army***. Carlisle Barracks, PA: Army War College, 2004. 43p.
Abstract: The old paradigms of U.S. military operations in the industrial age are dead. Military relevance in the information-dominated 21st Century no longer comes from the industrial age concept of massing forces or attrition warfare. Rather, it comes from a new information age paradigm in which access to information enables the rapid employment of the right force at the right place and time to achieve strategic objectives, while preventing any adversary from doing the same. To achieve this position of dominance, the Department of Defense has embraced the concepts of Network Centric Warfare (NCW) as a way to transform the force and achieve Joint Vision 2020 objectives. This information age concept provides a systems view of the battle space that can radically compress the strategic, operational, and tactical levels of war and dramatically increase combat power through shared awareness and self-synchronization. The concept will not take hold in the U.S. Army, however, without a substantial effort to overcome impediments and a corresponding co-evolution of processes, organizations, and technology infrastructure. This research paper provides a summary of network centric warfare concepts and highlights some of the challenges of applying them throughout a transformed Army force.
ACCESSION NUMBER: ADA423794
http://handle.dtic.mil/100.2/ADA423794

Quinn, Timothy W. ***Can We Get There From Here? RMAs, Network-Centric Warfare and the Process of Transformation***. Newport, RI: Naval War College, February 1999. 25p.

Abstract: *Among the hot buzzwords in U.S. military circles at present are the Revolution in Military Affairs (RMA) and Network Centric Warfare (NCW). RMA enthusiasts and technocrats argue that by harnessing emerging information technologies the U.S. can achieve Information Dominance in the battlespace of tomorrow, and fundamentally change the nature of warfare. The RMA is comprised of three elements: technology, doctrine, and organizational adaptation encompassed in the perceived strategic context. Network Centric Warfare envisions the combination of advanced sensors, weapons, and C4I systems from geographically dispersed units networked together into a continuously evolving ecosystem to create a whole greater than the sum of its parts. The results are forces achieving the massing of effects versus the massing of forces, operating with increased speed and synchronized from the bottom up to lock out enemy options while locking in success. Although the means of conducting war will change, the nature of it will not. The key to successfully formulating, implementing, and realizing any RMA will be the investment of our intellectual capital along the path. There is no such thing as the foreseeable future and we must not lock ourselves into a course with no allowable deviation but rather critically assess the who, what when, why, where and how as we move into the 21st century. We cannot wait for someone else to solve the problems for us rather we must all be involved to get there from here.*

ACCESSION NUMBER: ADA363146

http://handle.dtic.mil/100.2/ADA363146

Randall, Bobbie L. ***Sun Tzu: The Art of Network Centric Warfare***. Carlisle Barracks, PA: Army War College, 2001. 40p.

Abstract: *To meet the challenges of the future, the United States must have a strategy to ensure the joint force of tomorrow will be able to achieve full spectrum dominance. Joint Vision 2020 (JV2020) provides the Chairman, Joint Chiefs of Staff's vision of 21st century military operations and describes America's future military capability objectives. As our long-term objectives are evolving, however, so is our ability, from a technological and organizational perspective, to meet those objectives. Network Centric Warfare (NCW) provides the potential for significantly enhanced resources and instruments through which these objectives can be achieved. However, organizations (especially military organizations) often find it difficult to translate radically new resources into required capabilities. For this, we need a roadmap linking the development of future capabilities to future objectives. Sun Tzu, the ancient Chinese military philosopher, provides this necessary linkage. This paper examines the realization of JV2020 future military capability objectives (ends) by using Sun Tzu's timeless warfighting principles (ways) to guide the use of evolving NCW technologies and organizations (means).*

ACCESSION NUMBER: ADA389680

http://handle.dtic.mil/100.2/ADA389680

Read, Derek W. ***The Abbott and Costello Effect: Who's on What, and What's Where When? A Human-Centered Method to Investigate Network Centric Warfare Systems.*** Monterey, CA: Naval Postgraduate School, 2007. 71p.

Abstract: *Technological advancements, especially in communications systems, have led to a burgeoning interest in network centric warfare (NCW), fundamentally changing how warfare is being conducted. Network centric warfare (NCW) systems are being rushed to the field and are offered as a solution for the fog of war and as a way to reduce manpower costs. To date, there are no empirical findings that support or refute these NCW system claims. The goal of this thesis was to ascertain the utility of the Geographical Recall and Analysis of Data in the Environment (GRADE) as a method and process by which complex human-technological systems can be assessed. The GRADE builds upon the Dynamic Model of Situated Cognition (DMSC). This study essentially determines if GRADE could be used in model validation in laboratory and field settings for evaluating NCW claims. Unfortunately, that research goal was not entirely realized due to constraints and limitations in the data collection exercise. The thesis discusses the lessons learned from this research effort and makes recommendations about*

future exercises and how to better populate the DMSC with data. Additional recommendations for changes to the processes and procedures for data collection are provided.

ACCESSION NUMBER: ADA474389

http://handle.dtic.mil/100.2/ADA474389

http://bosun.nps.edu/uhtbin/hyperion-image.exe/07Sep%5FRead.pdf

Reynolds, Linda K. ***A Framework for the Management of Evolving Requirements in Software Systems Supporting Network-Centric Warfare.*** Monterey, CA: Naval Postgraduate School, 2006. 121p.

Abstract: Network-centric warfare (NCW) has changed the way the Department of Defense addresses technological improvements for its military forces. No longer is the emphasis on enhancing the capabilities of a single platform, but the focus is now on networking people, processes and technology to enable knowledge sharing and rapid decision-making. The capabilities required to support network-centric operations (NCO) in the NCW environment must be supported by new, innovative networked communication technologies. There are many sources of requirements for these software systems supporting NCO, which may increase in number as the Services continue to develop the capabilities necessary for the transformation to a fully networked military force. Requirements may also emerge and continue to evolve following the fielding of a NCO capability because new technology has the potential to change how warfighters work. Requirements evolution results in requirements engineering challenges associated with the acquisition and development of network-centric software systems. As such, an approach is needed to provide for consistency in elicitation, management and documentation of evolving requirements for technological capabilities supporting NCO. The purpose of this research is to address the problem of evolving requirements. The requirements engineering framework proposed by this thesis incorporates classification theory and requirements modeling principles, and is supported by the Extensible Markup Language (XML) family of technologies. Particular attention has been paid to the selection of nonproprietary, platform independent technology to ensure data can be exchanged between organizations. The framework demonstrates a means by which requirements can be classified and structured in a standardized format.

ACCESSION NUMBER: ADA457597

http://handle.dtic.mil/100.2/ADA457597

http://bosun.nps.edu/uhtbin/hyperion-image.exe/06Jun%5FReynolds.pdf

Roberts, David W. and Joseph A. Smith. ***Realizing the Promise of Network-Centric Warfare***. Norfolk, VA: Joint Forces Staff College, 2003. 26p.

Abstract: In the January 2003 issue of the United States Naval Institute's Proceedings, Dr. Milan Vego, Professor of Operations at the Naval War College, warns, "Network Centric Warfare (NCW) increasingly is becoming a new orthodoxy - a set of beliefs that cannot seriously be challenged."1 He and many other critics contend that NCW theorists fail to consider "Clause-witzian thoughts on the nature of war, the relationship between policy and use of military power, and the effect of fog of war and friction."2 They lament the perceived emphasis on tactics and targeting to the apparent exclusion of operational art, and warn that command and control (C2) is becoming increasingly centralized.3 What they don't say is that NCW is a bad idea, that it is unachievable, or that there is an alternate path for the transformation of the Defense Department advocated by the current administration. One look at the Secretary of Defense's transformation plan (including his choice for heading the Office of Transformation), at recent defense authorization figures, or at any of the emerging joint and Service operational concepts will confirm that NCW plays a prominent (if not dominant) role in the reshaping of the military.

ACCESSION NUMBER: ADA421630

http://handle.dtic.mil/100.2/ADA421630

Saunders, Clayton D. ***Al Qaeda: An Example of Network-Centric Operations***. Newport, RI: Naval War College, 2002. 24p.

Abstract: On 11 September 2001, Al Qaeda used information and knowledge advantage, access, and the ability to support forward-based teams, to conduct effects-based operations against the United States. Although obviously not employing the theory, in practice these operations appear to have been network-centric in nature, with Al Qaeda reaping the benefits inherent in this organizational and operational structure to conduct its attacks. Since VADM Cebrowski and John Garstka's January 1998 article, "Network Centric Warfare: Its Origin and Future," many defense related professional journals have continued the discussion, defining network-centric operations, describing their benefit to the fighting force and explaining how to develop the capability. But the discussion goes far beyond the military. In recent years there has been a change in the structure of information and technology that makes more information available more rapidly. Al Qaeda, by the way it uses information technology has, in effect, become a network-centric organization. Although it is a very different organization than the U.S. military, or more specifically, the Commander-in-Chief (CINC) of a regional unified military command, an examination of Al Qaeda's structure and operations may yield useful examples of network-centric theory put into practice.

ACCESSION NUMBER: ADA401158
http://handle.dtic.mil/100.2/ADA401158

Scherrer, Joseph H. ***Risks and Vulnerabilities of Network-Centric Forces: Insights from the Science of Complexity***. Newport, RI: Naval War College, 2003. 27p.

Abstract: NCW relies heavily on complexity science concepts like complex adaptive systems self-organization and network effects to support its proponents' claims of decisive operational utility to the war fighter. While many commentators have critiqued NCW from the historical, national-strategic, and "human-centric" perspectives, little work has been done to analyze the science behind the concept. This despite the fact that leading scientists in the field of complexity science admit that much more work needs to be done before the science's relevance to organized human activities is definitively proven. With the U.S. staking so much on network-centric capabilities, it is vital that the purported benefits of NCW be balanced by a frank assessment of its risks and vulnerabilities in anticipation of adversary challenges. For a combatant commander, the effects of an adversary intent on neutralizing or denying NCW's advantage will be immediately felt in the operational battlespace. As part of the operational planning process, a combatant commander's planning staff must identify the critical vulnerabilities associated with network-centric forces and formulate courses of action that mitigate risk and ensure operational protection of vital NCW capabilities. The central thesis of this paper is that the use of network-centric forces introduces risks and vulnerabilities that affect a combatant commander's ability to conduct operational warfare. An analysis is presented that illustrates potential risks and vulnerabilities of NCW, and recommendations are made that might help a combatant commander and a joint planning staff cope with them.

ACCESSION NUMBER: ADA415474
http://handle.dtic.mil/100.2/ADA415474

Schroeder, Michael C. ***The Issue of Command and Control in Network Centric Systems***. Newport, RI: Naval War College, 2001. 24p.

Abstract: Network Centric Warfare (NCW) promises enormous military advantages including information superiority, self-synchronization and increased decision making speed. However, with these advantages comes the capacity of the operational commander to exert too much control over the tactical levels of his command. The problem with the operational commander becoming involved in the tactical level is two fold. First, the operational commander is not the most qualified to manage those systems at the tactical level. Second, when the operational commander is making decisions at the tactical level, he is not making operational decisions which will have greater reaching implications. This paper will focus on the role of Network Centric Warfare (NCW) with regard to the operational function of command and control. It will first review the concepts of NCW, command and control, and the concepts of decentralized and centralized controls. Then, with this foundation, recent examples will be examined to derive recommendations for organization, doctrine and human elements to achieve the optimum command and

control structure. Through implementation of these recommendations future command and control structure will ensure the benefits of NCW are maximized and the risk of micromanagement minimized.
ACCESSION NUMBER: ADA390188
http://handle.dtic.mil/100.2/ADA390188

Senenko, Christopher M. ***Network Centric Warfare and the Principles of War***. Norfolk, VA: Joint Forces Staff College, 2007. 66p.
Abstract: A central pillar of future warfighting concepts for the United States military is the idea of Network Centric Warfare (NCW). This new approach to military operations attempts to leverage Information Age innovations and apply them to the execution of warfare. Some advocates of this concept believe that it will change the character and nature of warfare, therefore, making the conventional concepts of warfare obsolete. The principles of war are another way of referring to the conventional concepts and character of warfare. The United States military has adopted a standardized series of principles which have stood the test of time and can be traced back to many of the classical theorists of warfare such as the Prussian strategic theorist Carl Von Clausewitz, and the ancient Chinese military thinker Sun Tzu. It is these principles that must be analyzed when determining whether or not NCW has radically altered the landscape of warfare. While NCW concepts are force enablers and will assist the military of the future in the execution of its mission, they do not radically alter the classical principles of warfare and for this reason they should not be considered the prime motivator for future resourcing and doctrinal decisions.
ACCESSION NUMBER: ADA468857
http://handle.dtic.mil/100.2/ADA468857

Slais, Thomas A., Jr. ***Some Principles of Network-Centric Warfare: A Look at How Network-Centric Warfare Applies to the Principles of War***. Newport, RI: Naval War College, February 1999. 27p.
Abstract: The principles of war are one of the most important and enduring facets of operational art. Network centric warfare, enabled by technology of the information age, is a new concept the U.S. is adopting in order to fight faster, cheaper and better in the 21st century. This analysis shows that network centric warfare applies to the principles of war specifically, the principles of mass, offensive, unity of command and security. With regard to mass, the information, sensor and engagement grids of network centric warfare, will enable dispersed forces to mass effects by coordinating location, identification and targeting information from sensors to rapidly employ long range, precision fires, using shared information from a common operational picture. With respect to offensive, network centric warfare will effectively allow us to dominate factor time and operate inside the enemy's decision cycle. Thus, it will enhance our ability to seize and retain the initiative and preserve our freedom of action. As it applies to unity of command, network centric warfare will aid tactical commanders, armed with a clearly defined commander's intent from the operational level, to maintain the situational awareness required to self synchronize and act on opportunities while maintaining unity of effort toward achieving the operational commander's objective. Finally, with regard to security, network centric warfare will increase our ability to achieve battle space dominance through information superiority. However, we will be increasingly dependent on protecting our C4I systems to ensure that we can achieve our military objectives. The tie that binds network centric warfare to the principles of war is that it will enable enhanced situational awareness, which will improve our ability to abide by the principles in a more sufficient manner.
ACCESSION NUMBER: ADA363055
http://handle.dtic.mil/100.2/ADA363055

Steadley, Robert S. ***Operational Meteorology and Oceanography and Network-Centric Warfare: Implications for the Joint Force Commander***. Newport, RI: Naval War College, Joint Military Operations Department, February 1998. 28p.
Abstract: After a number of years of exponential growth in the technologies of computing power and global wireless communications, the U.S. Navy has adopted Network Centric Warfare (NCW) as the latest

'Revolution in Military Affairs'. This concept has the potential for wide application in the joint arena, where the rapid rate of data and information assimilation, fusion, and dissemination offer the Joint Force Commander (JFC) the potential to achieve Dominant Battlespace Awareness. Adapting to a 'network-centric' environment should be a key focus of all DOD components, but particularly service organizations, such as meteorology and oceanography (METOC), who will be tasked to support an ambitious charter of network requirements. The components must therefore scrutinize current operations with an eye towards supporting the concept of network nodes, which would act as a control and fusion hubs for the vast amounts of data and information flowing into the network. These nodes would serve as focal points for the flow of full spectrum support across the range of warfighters operating in a particular Joint Operating Area (JOA). When applied to the joint arena, the JFC, through the assigned Joint METOC Officer (JMO) should assess the best location and composition of the supporting node, with respect to the nature of the assigned mission and JOA. This paper discusses a number of METOC node options available to the JFC.
ACCESSION NUMBER: ADA348418
http://handle.dtic.mil/100.2/ADA348418

Tay, Chee B. and Whye K. Mui. ***An Architecture for Network Centric Operations in Unconventional Crisis: Lessons Learnt from Singapore's SARS Experience***. Monterey, CA: Naval Postgraduate School, 2005. 101p.
Abstract: *Singapore and many parts of Asia were hit with Severe Acute Respiratory Syndrome (SARS) in March 2003. The spread of SARS lead to a rapidly deteriorating and chaotic situation. Because SARS was a new infection, there was no prior knowledge that could be referenced to tackle such a complex, unknown and rapidly changing problem. Fortunately, through sound measures coupled with good leadership, quick action and inter-agency cooperation, the situation was quickly brought under control. This thesis uses the SARS incident as a case study to identify a set of* ***network centric warfare*** *methodologies and technologies that can be leveraged to facilitate the understanding and management of complex and rapidly changing situations. The same set of methodologies and technologies can also be selectively reused and extended to handle other situations in asymmetric and unconventional warfare.*
ACCESSION NUMBERADA429839
http://handle.dtic.mil/100.2/ADA429839
http://bosun.nps.edu/uhtbin/hyperion-image.exe/04Dec%5FTay.pdf

Thomas, Jeffrey A. ***Evaluating the Claims of Network Centric Warfare***. Monterey, CA: Naval Postgraduate School, 2005. 103p.
Abstract: *In response to technological advances, Network Centric Warfare (NCW) emerged as a theory to leverage the technology available in today's world. Advocates of NCW claim that technology will improve information sharing by "&robustly networking a force", thereby improving mission effectiveness. This study proposes a methodology with which to test the first tenet of NCW: a robustly networked force improves information sharing. Lessons learned from Human Systems Integration (HSI) demonstrate that in order to improve mission effectiveness, characteristics of both the human and the technology must be considered. As such, the impact of human characteristics and traits on mission effectiveness, as measured by individual and team performance, are assessed using a computer simulation, C3Fire. Results at the individual level, suggest that persons scoring high on extraversion and low on pessimism perform better than those scoring low on extraversion and high on pessimism. In contrast, at the team level, homogenous teams as measured by optimism-pessimism performed worse than diverse teams. Results of this thesis provide a methodology with which to examine NCW's claims in a laboratory setting. Preliminary evidence demonstrates the need to consider human characteristics and traits in the design and composition of network teams.*
ACCESSION NUMBER: ADA443309
http://handle.dtic.mil/100.2/ADA443309
http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Dec%5FThomas.pdf

Thorne, Mike. ***Network Centric Warfare and the Changing Role of the Signal Corps***. Carlisle Barracks, PA: Army War College, 2004. 31p.

Abstract: This research paper will explore the missions and construct for Army future force information and knowledge management organizations as part of a network centric information infrastructure. The Network Centric Information infrastructure will herald in a new paradigm for the Army Signal Corps-it no longer will be just a communications provider. Through the implementation of enhanced technologies and the adoption of a network centric approach we can obviate the need for communications installers and maintainers on the future battlefield. This requires a vision predicated on dramatically changing the Signal Corps as we know it. We must begin with the end in mind and recognize that technology and new doctrine will allow us to move to this new paradigm. We can field a future force with embedded communications capabilities thereby allowing the Signal Corps to move into the arena of joint information and knowledge management. This will require specialized training but not a unique force to implement. We can mold Military Intelligence (MI) Information Operations (IO) and automation officers into a cohesive team of knowledge management professionals that will be the core of the new Signal Corps. Professional Army communicators must embrace new missions and define a new paradigm or find themselves in forced obsolescence. This paper will propose a feasible course of action that will facilitate the development of a network centric information infrastructure in support of the future force. Furthermore the paper will present the benefits of transforming the core mission of the Signal Corps to one of knowledge management in keeping with the overall implementation of a network centric system in an era of joint interdependence.

ACCESSION NUMBER: ADA424057

http://handle.dtic.mil/100.2/ADA424057

Valentine, Jennifer R. ***Application of the Strategic Alignment Model and Information Technology Governance Concepts to Support Network Centric Warfare.*** Wright-Patterson AFB, OH: Air Force Institute of Technology, 2006. 116p.

Abstract: This thesis analyzes the fields of E-Business and Network Centric Warfare (NCW) in order to identify gaps and overlaps within the two bodies of knowledge. Successful implementation of E-business is more than simply applying a technology to an existing business model. It is about evolving business processes and structures in order for the organization to accommodate for this new dynamic environment. This thesis proposes that while the two areas? success fundamentally resides in the implementation and exploitation of technology, it is only through sound IT Governance policies and strategic alignment practices that success can be measured. Technology has the ability to bring increased capabilities to the warfigther. This work suggests the Air Force must analyze the implications of technology to its current structure, policies and processes prior to implementation on the enterprise. This thesis presents how the Strategic Alignment Model, as developed by Henderson and Venkatraman, can be applied to Air Force operations in order to better align its IT and mission objectives. Finally, this thesis proposes a model of the components necessary to execute an E-Business model wihtin an organization and suggests the same components are necessary to execute NCW initiatives.

ACCESSION NUMBER: ADA453565

http://handle.dtic.mil/100.2/ADA453565

Vandegrift, Todd D. ***The Asymmetric Response to Network-Centric Lock-Out Strategies and the Escalation of Violence***. Newport RI: Naval War College, 2004. 27p.

Abstract: As the world's sole superpower, the United States will operate in an asymmetric environment for the foreseeable future. This asymmetric environment is ultimately defined by perceived differences in the will and means of the United States in relation to its opponents. Unable to compete with the United States militarily, the asymmetric enemy perceives his will to fight as his competitive edge. These perceptions underwrite enemy strategies aimed at eroding U.S. will to fight by exploiting what the enemy believes is a U.S. aversion to casualties. To deal with this emerging challenge, the U.S. military is adopting an effects-based approach aimed at striking the adversary's will to fight. Acting quickly and

decisively, effects-based strategies strive to "lock-out" or foreclose alternate enemy courses of action. However, the enemy's reaction must be considered as the operational commander employs these strategies. Given the opponent's dwindling opportunity for military action as a result of a "lock-out" strategy, he may be expected to escalate the level of violence on an increasing compressed time line. Asymmetric enemies may be expected to strike preemptively to dissuade or complicate U.S. military action. The use of force may be directed at U.S. military targets to increase U.S. casualties, or at other U.S. "opponents" to complicate or deter U.S. military involvement. To mitigate the effects of these enemy counter-efforts, the operational commander must focus on effective operational protection and accurate identification of enemy courses of action during the planning process.

ACCESSION NUMBER: ADA422734

http://handle.dtic.mil/100.2/ADA422734

Villa, Jiancarlo. ***Network Centric Warfare - A Tool or Hindrance to the Operational Commander***. Newport, RI: Naval War College, 2004. 27p.

Abstract: Network Centric Warfare has been identified as the manner in which the Joint Force will operate in the 21st Century. Six years after VADM Arthur Cebrowski proposed the road to a netted force, we are able to examine the progress toward the attainment of that goal. To achieve its goals of speed of command and self-synchronization of the forces, NCW integrates three grids into a combined picture aimed at simplifying the planning and execution processes. The information of these grids is merged into a common operating picture which is to be a coherent picture of the battlefield. Independent production and development of networks by the various branches of the military service has caused the COP to receive its information from systems which have been produced in a stove pipe' and don't truly integrate into the COP. The current challenge for the Joint Force is to achieve the ordered objectives with a smaller force while increasing speed and effectiveness of mission accomplishment. Network Centric Warfare must facilitate the Joint Force Commander's achievement of the Joint Vision 2020 mandate of full spectrum dominance and enable his expediency of command which is integral in the effective conduct of operations across the military spectrum. NCW architects are successfully proceeding to develop the tenets of speed of command and self synchronization by providing technologically advanced sensors and systems. However, they must not lose sight of the fact that NCW technology must enable operational art and aid in the commander's ability to synchronize fires and maneuver along with the available instruments of National Power to achieve the objective.

ACCESSION NUMBER: ADA422740

http://handle.dtic.mil/100.2/ADA422740

Warne, Leoni, et al. ***The Network Centric Warrior: The Human Dimension of Network Centric Warfare***. Salisbury, Australia: Defence Science and Technology Organiation, Information Sciences Laboratory, 2004. 106p.

Abstract: Much of the NCW related work done by the military has been in technological and operational domains. The literature review in this report focuses on the human and organisational factors that need to be considered to make the most of the future NCW context and enable future warfighters to deal with war, peace, terrorism and overall uncertainty. Particular focus is placed on the transformation of warfighting and the issues that individuals and groups face in the NC environment. Such issues include: organisational culture, cognitive demands, the nature of information, C2 processes, knowledge mobilisation and learning, and transformational pathways organisations may follow while changing from a traditional hierarchical way of operating to more flexible and decentralised structures. The report concludes with suggestions for future research in the human dimension of effective NCW.

ACCESSION NUMBER: ADA426720

http://handle.dtic.mil/100.2/ADA426720

Washington, Julius C. ***Network Centric Warfare and Command and Control: Rethinking Organizational Architecture***. Newport, RI: Naval War College, 2001. 26p.

Abstract: We know from history that the ability of a military commander to effectively control his forces was forever changed by the French Revolution and the levee en masse. Thereafter, the sheer size and dispersion of forces made it necessary to subdivide them, and eventually to institute a rigid organizational system that has become increasingly more complex. Communications became extremely difficult with the available signal technology, making it almost impossible to synchronize these widely dispersed forces. The subsequent arrival of the telegraph vastly improved military communications, and today forces of almost unlimited size and separation routinely share information and intelligence in near-real time. From the late 20th century explosion in information and computing technology emerges the concept of Network Centric Warfare. Network Centric Warfare applies the vast potential of the Information Age to warfare, envisioning a netted battle force executing high-speed, synchronized operations with precise effect. Rich, scalable visualizations that reflect all relevant factors in the battlespace, or Common Operating Pictures (COPs) as they have been coined, become the essential element of United States military power in the 21st century.

ACCESSION NUMBER: ADA393553

http://handle.dtic.mil/100.2/ADA393553

Wells, David P. ***Managing the Double Edged Sword of Network-Centric Warfare***. Newport, RI: Naval War College, 2003. 17p.

Abstract: Network Centric Warfare can tend to collapse the operational level war by allowing information to flow around or past hierarchical staff structures and directly between tactical and strategic level decision makers. Why this has benefits in that it may streamline decision-making and reduce staff sizes, it can have serious detrimental impacts on joint warfare. Fortunately, by employing developed Information Management techniques during planning disciplined staffs can develop methods that will enhance the positive benefits of Network Centric Warfare while negating many of its serious drawbacks and weaknesses.

ACCESSION NUMBER: ADA415422

http://handle.dtic.mil/100.2/ADA415422

West, Paul D. ***Network-Centric System Implications for the Hypersonic Interceptor System***. West Point: NY: Military Academy, 2005. 51p.

Abstract: This report identifies the qualities and attributes of network-centric (NCS), describes a taxonomy of 13 critical NCS risk factors, and outlines a value-based model for NCS risk management, all as they affect the operation of a hypersonic interceptor (HSI) system. Successful employment of an HSI system requires a thorough integration of operations into the larger NCS super-system. Required capabilities previously identified for an HSI indicate the intent for this system is to function in full collaboration with the Joint Exercise Support System Intelligence Module(JIM), Unit of Employment (UE), and Unit of Action (UA) forces, which will operate in a network-centric framework. Based on these required capabilities and the common NCS factors, it is recommended that the Hypersonic Interceptor IPT identify specific measures of effectiveness (MOE) relevant for system risk management in an NCS environment and incorporate these measures and the methodology described in this report into the system life-cycle management plan. Specific actions to implement these recommendations include the development of a decision support tool to assess key stakeholder risk profiles and to model attribute weights in pre- and ongoing HSI operations, development of MOE to assess ongoing and post-operations analysis, and collaboration with engineers and operators of related NCS node programs.

ACCESSION NUMBER: ADA434078

http://handle.dtic.mil/100.2/ADA434078

White, Orrick. ***Network Centric Operations: Challenges Associated with the Human-in-the-Loop***. Ottawa, Canada: Defence Research and Development Centre, 2005. 31p.

Abstract: The human-system interface is central for achieving Network Centric Operations (NCO). Without systems that are designed to be human-centric, NCO will be a "non-starter." Given this reality, studies of command and control compatibility between human operators and the network are crucial. Without this human-oriented focus, unintended consequences will inevitably occur. Unfortunately, this would be just what the gurus of network-centric operations were trying to overcome.

ACCESSION NUMBER: ADA436359

http://handle.dtic.mil/100.2/ADA436359

Williamson, Ahmed T. ***Analyzing the Effects of Network Centric Warfare on Warfighter Empowerment.*** Monterey, CA: Naval Postgraduate School, 2002. 173p.

Abstract: NCW is a conceptual warfighting paradigm that seeks to exploit the advantages of information technologies to develop information superiority, leading to battlefield awareness and later escalating to battlefield dominance during future military operations. While military forces are currently experimenting within the framework of this new concept, efforts are being made to harness the opportunities made available by implementing network-centric concepts to increased operational efficiency and enhance combat power effectiveness so that optimal desired results may be achieved. However, the modem Marine Corps is comfortable and quite successful implementing its current, subordinate empowering doctrine of Maneuver Warfare, which emphasis the human behavioral aspects of warfare over technology implementation. The issue, then, is: how will Marine Corps warfighting performance be affected by changes in doctrine driven by advances in and the implementation of technology. This thesis seeks to answer this question through exploratory research of theoretical concepts on organizational performance, an examination of current and future warfighting concepts, and an assessment of the practicality of successfully implementing future warfighting concepts based upon the principles of a theoretical framework. Recommendations are provided for creation of a metro that will adequately assess the performance of empowered warfighters in a Network Centric Warfare environment.

ACCESSION NUMBER: ADA

http://handle.dtic.mil/100.2/ADA405963

Witsken, Jeffrey R. ***Network-Centric Warfare: Implications for Operational Design***. Fort Leavenworth, KS: Army Command and General Staff College, 2002. 64p.

Abstract: The United States military is adapting itself to fight warfare in the Information Age, preparing forces that use information superiority as a key weapon. Advocates of this communication-based and information-based form of warfare use the term 'Network-Centric Warfare' to describe the new paradigm. This new form of warfighting is expected to fully exploit the power of shared information and superior communications. Both of the recent 'Joint Vision' documents, Joint Vision 2010 and Joint Vision 2020, embrace this new form of warfare as a central feature of the future of the U.S. military. But does Network-Centric Warfare significantly alter operational design of a campaign? Network-Centric Warfare is essentially warfare that generates combat power by effectively linking (networking) actors, sensors, and decision-makers. Shimon Naveh's definition of a campaign (as the competition of two competing complex systems) helps frame the context and relevance of Network-Centric Warfare. Given this context, one cannot underestimate the central importance of the sensor network to the overall effectiveness of the networked force. A campaign planner must consider the abilities and limitations of his sensor network as he plans the campaign, and design appropriate actions accordingly. Additionally, the campaign planner must carefully balance dispersion and mass to counter erosion of forces and sustain operational momentum. A campaign plan must contain the right balance of Network-Centric Warfare and traditional means to attain operational objectives.

ACCESSION NUMBER: ADA403832

http://handle.dtic.mil/100.2/ADA403832

Woodcock, Al. ***The JFACC in a Network Centric World***. Newport, RI: Naval War College, 2001. 30p.

Abstract: The current Joint Forces Air Component Command (JFACC) command and control (C2) structure is rapidly becoming cumbersome and unable to meet the challenges of modern warfare. The infrastructure and manning required to meet the needs of command and control of the air are too large. The current processes involved in the control of air assets are excessively lengthy and unresponsive. These processes limit the flexibility and speed of modern aircraft and sensors. Network Centric Warfare (NCW) holds the promise of mitigating many of the current shortfalls in the system. Through networking and reachback principles, NCW will allow geographically dislocated entities to function as one organization. This ability enables JFACC staffs to become more agile and adaptable. it also facilitates the distribution of control to decision makers who can rapidly analyze, decide and act in given situations, thereby enabling a pace of operations not previously possible.. All of this will allow the JFACC to more efficiently and effectively employ airpower than ever before.

ACCESSION NUMBER: ADA389589

http://handle.dtic.mil/100.2/ADA389589

Psychological Warfare

Books

Barnett, Frank R and Carnes Lord. (eds.) **Political Warfare and Psychological Operations: Rethinking the U.S. Approach**. Washington, DC: National Defense University Press, 1989. 242p.
http://purl.access.gpo.gov/GPO/LPS53194
DKL UB276 .P65 1989 GENERAL

Briscoe, Charles H., et al. **Weapon of Choice: ARSOF in Afghanistan**. Fort Leavenworth KS: Combat Studies Institute Press, 2004. 399p.
DKL D 110.2:AF 3 FEDDOCS

Cox, Lee-Volker. **Planning for Psychological Operations: A Proposal**. Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 79p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1061

Goldstein, Frank L. and Benjamin F. Findley (eds.). **Psychological Operations: Principles and Case Studies**. Maxwell Air Force Base, AL: Air University Press, 1996. 364p.
http://www.au.af.mil/au/aul/aupress/Books/Goldstein/Goldstein_B18.pdf
DKL UB276 .P82 1996 GENERAL

Hosmer, Stephen T. **Psychological Effects of U.S. Air Operations in Four Wars, 1941-1991: Lessons for U.S. Commanders.** Santa Monica, CA: RAND, 1996. 220p.
http://www.rand.org/pubs/monograph_reports/2005/MR576.pdf
DKL UG632 .H67 1996 GENERAL

Hosmer, Stephen T. "The Information Revolution and Psychological Effects." p. 217-251, IN: Khalilzad, Zalmay and John White (eds.) **Strategic Appraisal: The Changing Role of Information in Warfare**. Santa Monica, CA: Rand, 1999. 452p.
http://www.rand.org/pubs/monograph_reports/MR1016/index.html
DKL UG478 .C43 1999 GENERAL

Johnson, Richard Denis. **Seeds of Victory: Psychological Warfare and Propaganda: The Seeds of Victory in Modern Political & Military Campaigns: The Persian Gulf War as a Case Study in Operational Principle**. Atglen, PA: Schiffer Pub., c1997. 283p.
DKL DS79.744 .P78 J64 1997 REFERENCE

Kriesal, Melvin E. "Psychological Operations: A Strategic View." p. 53-103, IN: **Essays on Strategy**. Washington, DC: National Defense University Press, 1985.
DKL U162 .E77 1985 GENERAL

Raevsky, Andrei. **Managing Arms in Peace Processes: Aspects of Psychological [Operations] and Intelligence**. UNIDIR/96/31. New York: United Nations, 1996. 46p.

Roberts., M.E. **Villages of the Moon: Psychological Operations in Southern Afghanistan**. Baltimore, MD: Publish America, 2005. 207p.

Rothstein, Hy S. "Strategy and Psychological Operations." p. 160-186 IN Arquilla, John and Douglas A. Borer (eds.). **Information Strategy and Warfare: A Guide to Theory and Practice**. New York: Routledge, 2007. 248p.
DKL U163 .I54 2007 GENERAL

Thomas, Timothy L. **The Russian PSYOP and Information Operations Interface**. Ft. Leavenworth, KS: Foreign Military Studies Office, 1996. 12p.
http://www.au.af.mil/au/awc/awcgate/fmso/psyop.htm

United States. Department of the Army. **Psychological Operations Leaders Planning Guide**. GTA 33-01-001. [Washington, DC:]: U.S. Army Training Support Centers, 2005.
http://www.fas.org/irp/doddir/army/psyopplan.pdf

United States. Joint Chiefs of Staff. **Doctrine for Joint Psychological Operations.** Joint Pub 3-53. Washington, DC: Joint Chiefs, 2003.
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_53.pdf

United States. Joint Chiefs of Staff. **Military Deception**. Joint Pub 3-13.4. Washington, DC: Joint Chiefs, 2006.
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_4.pdf

Periodicals

Adams, Thomas K. “Psychological Operations in Bosnia.” **Military Review**, December 1998-February 1999, v. 78, no. 6, p. 35-36.

Alexander, Mark T. “Getting the Word Out: The Role of PSYOP in the ACRI.” **Special Warfare**, Summer 1998, v. 11, no. 3, p. 18-21.

Belknap. Margaret H. “The CNN Effect: Strategic Enabler or Operational Risk?” **Parameters**. Autumn 2002, v. 32, no. 3, p. 100-114. *http://www.carlisle.army.mil/usawc/Parameters/02autumn/belknap.pdf*

Blanchette, Joel G. “USACAPOC's (Army Civil Affairs and Psychological Operations Command) FOCUS Project: Waging the War for Information.” **Special Warfare**, January 1996, v. 9, no. 1,p. 45-49.

Boisselle, James C. "Tactical PSYOPs Supporting the Infantry Brigade and Battalion." **Infantry**, September/October 1996, v. 86, no. 5, p. 14-17.

Bowdish, Randall G. “Information-Age Psychological Operations.” **Military Review**, December 1998-February 1999, v. 78, no. 6, p. 29-35.

_____. "Psychological Operations...From the Sea." **United States Naval Institute Proceedings**, February 1998, v. 124, no. 2, p. 70-72.

Boyd, Curtis D. “A Unique Organization: The 3rd Battalion, 1st Special Warfare Training Group.” **Special Warfare**, August 2003, v. 16, no. 2, p. 12-18.

_____. “Army IO is PSYOP: Influencing More with Less.” **Military Review**, May/June 2007, v. 87, no. 3, p. 67-75. *http://usacac.army.mil/CAC/milreview/English/MayJun07/Boyd.pdf*

_____. “CA and PSYOP: Major Changes in Personnel, Training Upcoming for Officers, NCOs.” **Special Warfare**, July 2005, v. 18, no. 1, p.20-23.

Briscoe, C.H. “Coalition Humanitarian Liaison Cells and PSYOP Teams in Afghanistan.” **Special Warfare**, September 2002, v. 15, no. 3, p. 36-38.

_____. “Wanted Dead or Alive: Psychological Operations During Balikatan 02-1.” **Special Warfare**, September 2004, v. 17, no. 1, p. 26-29.

Brooks, Paul, R.M., Jr. “A Vision for PSYOPS in the Information Age.” **Special Warfare**, Winter 2000, v. 13, no. 1, p. 20-24.

Brown, Stephen D. “PSYOP in Operation Uphold Democracy.” **Military Review**, September/October 1996, v. 76, no. 5, p. 57-64.

Burton, Janice. “PSYOP Transformed.” **Special Warfare**, September/October 2006, v. 19, no. 5, p. 10-13.

Centner, Christopher M. "Precision-Guided Propaganda: Exploiting the U.S. Information Advantage in Peacetime." **Strategic Review**, Spring 1997, v. 25, no. 2, p. 35-41.

Collins, Steven. “Army PSYOP in Bosnia: Capabilities and Constraints.” **Parameters**, Summer 1999, v. 29, no. 2, p. 57-73.
http://carlisle-www.army.mil/usawc/Parameters/99summer/collins.htm

_____. “’Centrally Planned and Decentrally Executed’ – A Dilemma Facing Military Psychological Operations.” **Cyber Sword**, Fall 1999, v. 3, no. 1, p. 19-21.

_____. “NATO and Strategic Psyops: Policy Pariah or Growth Industry.” **Journal of Information Warfare**, 2002, v. 1, no. 3, p. 72-78.
http://ics.leeds.ac.uk/papers/pmt/exhibits/32/JIW1_32.pdf

Copley, Gregory. “PsyOps is a Distinct, but Integral, Part of Information Warfare.” **Defense & Foreign Affairs Strategic Policy**, April 1997, v. 25, no. 5, p. 35.

Copley, Gregory R. “Re-Defining Psychological Strategy in the Age of Information Warfare.” **Defense & Foreign Affairs Strategic Policy**, June 1998, v. 26, no. 6, p. 5-8.

Crews, Fletcher. "PSYOP Planning and the Joint Targeting Process." **Special Warfare**, Winter 1998, v. 11, no. 1, p. 16-21.

David, G. John and E. Lawson Quinn. “A Tactical Staff Structure for an Ideological War.” **Marine Corps Gazette**, February 2006, v. 90, no. 2, p. 30-32.

D’Aoust, Maurice. “Hoodwinked: Confederate Military Deception Part 2.” **Civil War Times Illustrated**, June 2006, v. 45, no. 4, p. 42-48.
http://www.historynet.com/magazines/civil_war_times/3038701.html

_____. “Hoodwinked: Union Military Deception.” **Civil War Times Illustrated**, May 2006, v. 45, no. 3, p. 34-39.
http://www.historynet.com/historical_conflicts/3446521.html

Dobrydney, John F. “Marine Tactical PsyOp Teams.” **Marine Corps Gazette**, February 2006, v. 90, no. 2, p. 33-35.

Duffy, Dave. “UW Support to Irregular Warfare and the Global War on Terrorism.” **Special Warfare**, May/June 2007, v. 20, no. 3, p. 12-15.

Dyer, Mark F. “Theory, Research, Practice: Three Ways to Increase PSYOP Effectiveness.” **Special Warfare**, Fall 1999, v. 12, no. 4, p. 24-30.

Emery, Norman, Jason Werchan and Donald G. Mowles, Jr. “Fighting Terrorism and Insurgency: Shaping the Information Environment.” **Military Technology**, November 2006, v. 30, no. 11, p. 104-110.

Friedman, Herbert A. “Falling Leaves.” **Print**, September/October 2003, v. 57, no. 5, p. 80-87.

Goldmann, Jeanne and Fran Landy. “Officer Professional Development: Psychological Operations Functional Area. **Special Warfare**, February 2004, v. 16, no. 3, p. 13-17.

Goldstein, Frank L. “Psychological Operations and Information Operations: A Perfect Union.” **Cyber Sword**, Fall 1999, v. 3, no. 1, p. 13-16.

Goldstein, Frank L. and Atilio M. Usseglio. “Psychological Operations Through Computer Networks.” **Cyber Sword**, Spring 2000, v. 4, no. 1, p. 21-23.

Guevin, Paul R. “Psychological Operations.” **Air & Space Power Journal**, Summer 2004, v. 18, no. 2, p. 30.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj04/sum04/guevin.html

Guy, John C. and Steven Collins. Current Challenges and Possible Roles for Army Reserve PSYOP Forces.” **Special Warfare,** Summer 2000, v. 13, no. 3, p. 28-35.

Hampsey, Russel J. “Voices from the Sierra Maestra: Fidel Castro's Revolutionary Propaganda.” **Military Review**, November/December 2002, v. 82, no. 6, p. 93-98.
http://usacac.army.mil/CAC/milreview/English/NovDec02/NovDec02/bob.pdf

Huhtinen, Aki and Jari Rantapelkonen. “Perception Management in the Art of War. A Review of Finnish War Propaganda and Present-Day Information Warfare.” **Journal of Information Warfare**, October 2002, v. 2, no. 1, p. 50-58.

Huss, Maj Jon. "Exploiting the Psychological Effects of Airpower: A Guide for the Operational Commander." **Aerospace Power Journal**, Winter 1999, v. 13, no. 4, p. 23-32.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/win99/huss.pdf

Hutchinson, William. “A Critique of Coalition Propaganda before the Second Gulf War.” **Journal of Information Warfare**, 2004, v. 3, no. 2, p. 29-41.

Jacobs, Jeffery A. “Civil Affairs in the Assault.” **Military Review**, September-October 1996, v. 76, no. 5, p. 65-73.

Jones, Craig S. “The Perception Management Process.” **Military Review**, December 1998-February 1999, v. 78, no. 6, p. 38-43.

Jones, Jeffrey B. “Theater Information Strategies.” **Military Review**, November 1994, v. 74, no. 11, p. 48-50.

Jones, Jeffery B. and Michael P. Mathews. “PSYOP and the Warfighting CINC.” **Joint Force Quarterly**, Summer 1995, no. 8, p. 28-33.
http://www.dtic.mil/doctrine/jel/jfq_pubs/1520.pdf

Kellogg, Robert H. “Evaluating Psychological Operations: Planning Measures of Effectiveness.” **Special Warfare**, May 2004, v. 16, no. 4, p. 32-37.

Kiper, Richard L. “'Of Vital Importance': The 4th PSYOP Group.” **Special Warfare**, September 2002, v. 15, no. 3, p. 19-21.

_____. “To Educate and to Motivate: The 345th PSYOP Company.” **Special Warfare**, September 2002, v. 15, no. 3, p. 32-33.

Knights, Michael. “US Psyops Escalate Against Iraq.” **Defense & Foreign Affairs Strategic Policy**, January/February 2003, v. 31, no. 1/2, p. 11+

Labash, Matt. “Psyching Out the Taliban.” **The Weekly Standard**, December 24, 2001, v. 7, no. 15, p. 25-27.

Lena, Jennifer C. “Psyops, Propaganda and Gangsta Rap.” **Radical Society**, April 2003, v. 30, no. 1, p. 25-30.

Lord, Carnes. “PSYOP and the Revolution in Military Affairs.” **Special Warfare**, Summer 1997, v. 10, no. 3, p. 28-34.

Lungu, Angela Marie. “WAR.com: The Internet and Psychological Operations.” **Joint Force Quarterly: JFQ**, Spring/Summer 2001, no. 28, p. 13 -17.
http://www.dtic.mil/doctrine/jel/jfq_pubs/0628.pdf

McElroy, David M. “Psyop – the Invisible Battlefield.” **Military Intelligence Professional Bulletin**, July-September 1990, v. 16, no. 3, p. 22-25.

Mills, John. “PSYOP: Radio Operations in Bosnia: A Steady, Positive Drumbeat.” **Special Warfare**, Fall 2001, v. 14, no. 4, p. 30-39.

Murray, Laura K. "China’s Psychological Warfare.” **Military Review**, September/October 1999, v. 79, no. 5, p. 13-20.

Myskey, Rick N. “ARAC: Transforming the Way Soldiers Think.” **Special Warfare**, March/April 2007, v. 20, no. 2, p. 30-31.

Nichol, James P. "Soviet Propaganda and Active Measures." **Problems of Communism**, January-February 1990, v. 39, no. 1, p. 93-100.

Parry-Giles, S. “The Eisenhower Administration’s Conceptualization of the USIA: The Development of Overt and Covert Propaganda Strategies.” **Presidential Studies Quarterly**, Spring 1994, v. 24, no. 2, p. 263-276.

Post, Jerrold M. “Psychological Operations and Counterterrorism.” **Joint Force Quarterly: JFQ**, 2nd Quarter 2005, no. 37, p. 105-110. *http://www.dtic.mil/doctrine/jel/jfq_pubs/1837.pdf*

“Psychological Strategy is Not Information War.” **Defense & Foreign Affairs Strategic Policy**, September 1997, v. 25, no. 9, p. 14.

Reid, R. Pierce. “Waging Public Relations: A Cornerstone of Fourth-Generation Warfare.” **Journal of Information Warfare**, 2002, v. 1, no. 3, p. 51-64. *http://ics.leeds.ac.uk/papers/pmt/exhibits/32/JIW1_32.pdf*

Robinson, Linda. “The Propaganda War: The Pentagon’s Brand-New Plan for Winning the Battle of Ideas Against Terrorists.” **U.S. News & World Report**, May 29, 2006, v. 140, no. 20, p. 29-31.

Rusnok, Richard M., Jr. "Get Psyched!" **United States Naval Institute Proceedings**, July 1998, v. 124, no. 7, p. 70-71.

Schleifer, Ron. “Psychological Operations: A New Variation on an Age Old Art: Hezbollah versus Israel.” **Studies in Conflict and Terrorism,** January/February 2006, v. 29, no. 1, p. 1-19.

Schoenhaus, Robert M. “The Application of National Power and the Role of Psychological Operations in the Information Age.” **Cyber Sword**, Fall 1999, v. 3, no. 1, p. 17-18.

Serookiy, Yu Ye. “Psychological-Information Warfare: Lessons of Afghanistan.” **Military Thought**, 2004, v. 13, no. 1, p. 196-200.

Shafer, Melvin E. "Attacking Through the MIST [Military Information Support Team]." **Military Review**, March/April 1996, v. 76, no. 2, p. 76-78.

Smyczek, Peter J. “Regulating the Battlefield of the Future: The Legal Limitations on the Conduct of Psychological Operations (PSYOP) Under Public International Law.” **The Air Force Law Review**, 2005, v. 57, p. 209-240.

Stankiewicz, Paul R. “Psyop: Winning Wars by Saving Lives.” **Asia-Pacific Defence Forum**, Winter 1992-1993, v. 17, no, 2, p. 8-14.

Starunskiy. A.G. “Psychological Operations of U.S. Military Services at the Present Stage.” **Military Thought** 2003, v. 12, no. 4, p. 162-171.

Steele, Dennis. “PSYOP in Bosnia: Prime-time Competition.” **Army**, March 1999, v. 49, no. 3, p. 31+

Stevenson, Jonathan. “’Special’ Forces.” **The National Interest**, November/December 2006, no. 86, p. 73-78.

Stonehill, Paul. "Soviet Psychic Warfare." **Fate**, February 1994, v. 47, no. 2, p. 70+

Szeredy, J. ‘Spyke’ “Influence Operations: Integrated PSYOP Planning.” **Air & Space Power Journal**, Spring 2005, v. 19, no. 1, p.38-44.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/spr05/szeredy.html

Thomas, Timothy L. “Human Network Attacks.” **Military Review**, September/October 1999, v. 79, no. 5, p. 23-33.

_____. “New Developments in Chinese Strategic Psychological Warfare.” **Special Warfare**, April 2003, v. 16, no. 1, p. 2-11.
http://fmso.leavenworth.army.mil/documents/chinesepsyop.pdf
http://www.iwar.org.uk/psyops/resources/china/chinesepsyop.pdf

_____. “Russian Information-Psychological Actions: Implications for U.S. PSYOP (Psychological Operations).” **Special Warfare**, Winter 1997, v. 10, no. 1, p. 12-19.
http://fmso.leavenworth.army.mil/documents/psyop/psyop.htm

Timmes, Thomas A. “Military Psychological Operations in the 1990s.” **Special Warfare**, January 1994, v. 7, no. 1, p. 19-21.

Tulak, Arthur N. “PSYOP C2W Information Operations in Bosnia.” **Call Training Techniques**, FY99, 2nd Quarter and **News From the Front!**, November/December 1998.

Vest, Jason. “Missed Perceptions.” **Government Executive**, December 2005, v. 37, no. 21, p. 68+
http://www.govexec.com/features/1205-01/1205-01s5.htm

Withington, Jonathan. “Practicing PSYOP.” **Soldiers**, October 2000, v. 55, no. 10, p. 8-9.

Documents, Theses & Technical Reports

Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography.

Acevedo, Dave. ***Strategic PSYOP: Coordinating Worldwide Psychological Operations - Is There a National Requirement for a Strategic Psychological Operations Organization?*** Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2003. 59p.

Abstract: *Psychological Operations (PSYOP) is a cornerstone of the United States' Information Operations and is a combat multiplier. As defined by Joint Doctrine, Psychological Operations (PSYOP) are operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. A Strategic PSYOP organization is necessary to breach the gap between diplomatic and political statements and actions and those statements and actions by military organizations. To be effective, PSYOP must operate in, with and amongst the national leadership and governmental organizations. Current operations in the Global War on Terror focus on the need to coordinate, integrate and conduct Psychological Operations at the strategic level. Throughout the 20th century, PSYOP has been a strategic enabler, enabling military and civilian forces to focus their efforts. PSYOP's importance has increased and decreased throughout the latter part of the century. The galvanizing events of September 11, 2001 bought a new focus to PSYOP and strategic information coordination. A Strategic PSYOP Unit will provide the focal point to coordinate various governmental organizations and national leadership directives into a cohesive, integrated PSYOP program. The majority of PSYOP expertise resides within that Army; however, manning a strategic PSYOP organization must be a joint endeavor. This provides for full participation from the Services, incorporating their unique capabilities. A joint strategic PSYOP organization will take time to implement, as the required skills and experiences must be grown throughout the Services. Ultimately, a Joint Strategic Psychological Operations Unit will provide the coordination and knowledge support required to the interagency and national leadership.*

ACCESSION NUMBER: ADA431000

http://handle.dtic.mil/100.2/ADA431000

Barger, Michael G. ***Psychological Operations Supporting Counterinsurgency: 4th Psyop Group in Vietnam.*** Fort Leavenworth, KS: Army Command and Staff College, 2007. 144p.

Abstract: *Military and civilian agencies conducted Psychological Operations on an unprecedented scale during the Vietnam War. Emphasis on PSYOP from MACV and the U.S. Mission resulted in the creation of an interagency organization providing direction to the overall PSYOP effort. The military PSYOP force supporting MACV underwent a series of organizational changes over seven years as the force struggled to meet ever-increasing demands, but never reached their full potential in Vietnam. Difficulties in measuring effectiveness combined with a lack of understanding of PSYOP techniques and capabilities more often than not resulted in the relegation of PSYOP to supporting 'sideshow' status rather than the full integration into supported unit planning necessary for success. However, the evolution of the PSYOP force and reports from participants provide numerous lessons learned applicable to current operations under the aegis of the Global war on Terrorism.*

ACCESSION NUMBER: ADA471075

http://handle.dtic.mil/100.2/ADA471075

Barucky, Jerry, Bryan Karabaich, and Brice Stone. ***Evaluation of Cross-Cultural Models for Psychological Operations: Test of a Decision Modeling Approach***. San Antonio, TX: Metrica Inc, 2001. 77p.

Abstract: Specific research objectives were to identify sample psychological operations (PSYOP) objectives likely to be sought in traditional wartime operations and from operations other than war; for two sample objectives, to identify cultural and situational factors that would influence a likelihood that a target audience (TA) would respond as desired; to determine if a policy-capturing methodology would result in a policy model that could assess the probability of a TA responding as desired under varying conditions; and to examine the degree that relationship of factors and TA response is consistent across cultures and situations. Comparisons of relative influence of factors across/within cultures showed moderate but inconsistent agreement between subjects/cultures. In general, decision analysis procedures proved to be easily implemented. From these results, there is strong indication that relevant influencing factors can be pre-identified for specific PSYOP objectives. However, additional research over a larger number of objectives/cultures is required to see if these results are generalized to different types of operations and target audiences.

ACCESSION NUMBER: ADA400796

http://handle.dtic.mil/100.2/ADA400796

Carter, Rosemary M. ***Information Operations Coordination Cell-Necessary for Division Offensive Actions***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, December 1998. 67p.

Abstract: This monograph analyzes the need for a division Information Operations (IO) Coordination Cell during offensive military actions. The integrated concept team draft of FM 100-6, Information Operations: Tactics Techniques and Procedures, includes a division Information Operations Coordination Cell. The cell is responsible for integrating the components of Information Superiority (IS) to defeat the enemy's command, control, computers, communications, intelligence, surveillance and reconnaissance (C4ISR) while protecting friendly C4ISR. Their focus is the Information Operations segment of IS that includes operational security (OPSEC), psychological operations (PSYOP), military deception, electronic warfare (EW), physical destruction, computer network attack (CNA), public affairs (PA), and civil affairs (CA). The monograph restricts the topic to Offensive IO, or IO that attacks the enemy commander's ability to achieve his objectives. Also, the monograph limits the type of military action to offensive. The monograph focuses on offensive actions, the primary action within offensive operations, because that is what the Army is designed for; fighting and winning wars. The monograph analyzes the IO tasks using three supporting research processes. First, it determines that only five of the tasks are necessary for Offensive IO: PSYOP, military deception, EW, physical destruction, and CA. The monograph then analyzes current doctrine and the heavy division Army of Excellence Table of Organization and Equipment (TOE) to determine the division's capabilities to execute the Offensive 10 tasks. Finally, the monograph uses these capabilities and doctrine to determine if the current division staff has the necessary staff mechanisms to conduct the Offensive IO tasks.

ACCESSION NUMBER: ADA366192

http://handle.dtic.mil/100.2/ADA366192

Cox, Lee-Volker. ***Planning for Psychological Operations A Proposal***. Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 91p.

Abstract: It is incumbent upon the state to gain support for national objectives. Employment of instruments of power is designed to influence other nations and organizations to respond favorably. Therefore, impacting the decision making process is the underlying principle for IOP power projection and highlights the psychological element. During a period of declining resources and increased world competition, the United States must find new ways to reach out and promote American interests. In order to maximize the impact and exploit the influence events create, joint planning and interagency coordination of psychological operations are critical. The current ad hoc interagency coordination and joint planning process do not maximize the psychological factors impact and fully exploit its asymmetrical

influence on a target audience audience's decision making process. Traditional views towards concepts, particularly military PSYOP, do not lead to the innovative solutions demanded by an environment of declining funds and resources. This study recognizes the multidimensional aspect of military PSYOP and calls for redefining an area of operations that has changed little over the years. Additionally, the establishment of an organization responsible for the development of a national marketing strategy integrating all IOPs to achieve objectives beyond the tactical level is advocated. Reviewing subject matter literature from the last forty years provided the project's basis for concepts relating to PSYOP and the Soviet missile gap deception case study. Internet searches, interviews, and recent literature brought current issues to light and developed a picture of U.S. organizations involved in influencing target audiences.

ACCESSION NUMBER: ADA398453

http://handle.dtic.mil/100.2/ADA398453

Dovey, Thomas C., Jr. ***Conduct of Information Operations by a U.S. Army Division While Participating in a Stability Action***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, December 1998. 55p.

Abstract: This monograph assesses the capability of a US Army Division conducting stability actions to plan and conduct Information Operations (IO) in accordance with the FM 100-6 coordinating draft, Information Operations: Tactics, Techniques and Procedures (FM 100-6CD) and Tactics, Techniques and Procedures (TTP) developed in recent stability actions. It identifies what 10 tasks a US Army Division must be able to plan and execute in stability actions. It addresses what resources are required to conduct those 10 tasks. The monograph then provides an assessment of the ability of the Division conducting stability actions to perform the required tasks. The monograph concludes that the Division is capable of planning and conducting information operations while conducting stability actions. However, this answer assumes that the Division receives its habitual Psychological Operations (PSYOP) support element. The monograph brings out shortcomings in current 10 doctrinal methods discusses new TTPs developed by divisions serving as TF Eagle in Bosnia Herzegovina and ends with recommendations for improving 10 doctrine and input for FM 100-6CD TTP CD.

ACCESSION NUMBER: ADA366180

http://handle.dtic.mil/100.2/ADA366180

Duff, Murray J. ***Are Current Psychological Operations Procedures Adequate in Information Warfare***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, April 1997. 54p.

Abstract: This monograph discusses the ability of Psychological Operations forces to conduct information operations. The army has begun to develop capabilities that allow it to fight more effectively in an information intensive environment. While some aspects of information warfare are conducted domestically, many are executed on foreign soil and involve extensive interaction with other governments, their population, non-governmental organizations, and international organizations. Each of these entities constitutes a potential target audience for psychological operations while executing information warfare. The US Army is compelled to rely upon psychological operations forces to fill vital support roles in the conduct of information warfare. In this monograph, psychological operations capabilities are measured using Operation Desert Shield/Storm as a case study and to a lesser extent, recent OOTW operations. Based on the successes and failures found in these examinations, the monograph draws conclusions as to the abilities of the psychological operations force to conduct information warfare.

ACCESSION NUMBER: ADA334511

http://handle.dtic.mil/100.2/ADA334511

Esarey, Clinton D. ***Media and the U.S. Army: You Don't Always Get What You Want; You May Just Get What You Need***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 1994. 58p.

Abstract: Recently, the Chief of Staff of the Army stated that the United States Army must successfully wield new information technologies to ensure land force dominance into the twenty-first century. Currently the Army is developing an Information Operations Concept that describes the framework for the Army to conduct information warfare; however, the concept only generically treats the dynamic to move information from the battlefield to external audiences such as the American people. Because the media-military relationship will be instrumental in acquiring and disseminating information to the American people, understanding and invoking a stable relationship is of enduring importance to the Army and the nation. Therefore, the purpose of this monograph is to examine the characteristics of the U.S. media--Army relationship in the twenty-first century.

ACCESSION NUMBER: ADA284136

http://handle.dtic.mil/100.2/ADA284136

Freeman, Bryan R. ***The Role of Public Diplomacy, Public Affairs, and Psychological Operations in Strategic Information Operations***. Monterey, CA: Naval Postgraduate School, 2005. 77p.

Abstract: Organizing for and conducting effective public affairs, public diplomacy, and psychological operations in support of national security objectives is a complex endeavor. In many instances, the desired psychological effects are contingent upon the efficiency of the organization conducting the programs and the development and dissemination of appropriate messages and themes. At present, the U.S. Government's ability to influence on a global scale is deficient due to fragmented organizational structure and underdeveloped doctrine relating to strategic influence. Duplication of efforts, inconsistent themes, and the lack of a long-term, strategically focused, integrated information strategy have been inhibitors to American foreign policy success. Following the terrorist attacks on September 11th, the U.S. Government and the American people have wondered why we have been unable to effectively influence the majority of the population in the Middle East. Since that time, the government has struggled with the question of how to both organize for and effectively conduct a strategic influence campaign in support of the Global War on Terror (GWOT). The United States' present capacity to conduct strategic influence in the Middle East is hindered by a dysfunctional organizational structure relative to strategic information operations and an institutional reluctance to recognize or value strategic influence as an effective instrument of statecraft. This thesis examines the three primary components of U.S. strategic influence: public diplomacy, public affairs, and psychological operations. Next is a look at various U.S. strategic information programs, their organizational structure, and the changes that have occurred in focus and policies from the beginning of the 20th century to the present. The final chapter examines public diplomacy, psychological operations, and public affairs as they relate to Operation Iraqi Freedom.

ACCESSION NUMBER: ADA435691

http://handle.dtic.mil/100.2/ADA435691

http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Jun%5FFreeman.pdf

Gallogly, Erin J. ***Nonlethal Information Operations Targeting Process: Duties, Responsibilities and Procedures***. Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, December 1998. 60p.

Abstract: This monograph's purpose is twofold. First, it provides the Joint Task Force Commander procedures by which to integrate nonlethal information operations into the joint targeting process and recommends duties and responsibilities for staff officers to ensure they integrate information operations into plans and operations. Second, it offers information operations officers a single document from which to develop standing operating procedures and tactics, techniques, and procedures. Joint Publications 3-0, Doctrine for Joint Operations, and 3-09, Doctrine for Joint Fire Support, provide the doctrinal underpinnings for joint targeting. Additionally, Joint Publication 3-13, Joint Doctrine for Information Operations, provides doctrine and guidance for information operations targeting. Currently there is neither

Army doctrine for information operations targeting nor tactics, techniques, and procedures on how to integrate information operations into the targeting process. This monograph attempts to fill this gap. The capabilities, limitations, and Employment considerations are outlined for the nonlethal information operations capabilities and activities (i.e., civil affairs, electronic warfare, military deception, psychological operations, public affairs, and special information operations). Finally, the author makes several recommendations in the areas of
personnel and organization, training and education, doctrine, and operations.

ACCESSION NUMBER: ADA366242

http://handle.dtic.mil/100.2/ADA366242

Goldstein, Frank L. and Benjamin F. Findley. ***Psychological Operations: Principles and Case Studies.*** Maxwell AFB, AL: Air University, 1996. 351p.

Abstract: *The scope of military PSYOP during World War II, the Korean War, and in much of the 1960s was primarily limited to combat propaganda and psychological warfare (psywar). During those times, it was accepted as a specialized tactical application and as a subordinate operation. The experiences of these conflicts, especially the Vietnam War, convinced some American military and political leaders that the psychological dimension of national power and conflict encompasses diverse elements and many activities-nonmilitary as well as military-in both peacetime and war in support of our national policy and objectives. Its scope can vary from the tactical battlefield to the operational theater to the strategic levels of conflict to national political and military goals. Part I serves as an introduction to the overall nature, historical background, and concepts of PSYOP, and to some principles that can be used for training in the field of psychological operations. The independent articles in this section reflect the broad range of historical development and thought about PSYOP and are intended to be a foundation for understanding the basic nature and key elements of PSYOP. Col Frank L. Goldstein, USAF, and Col Daniel W. Jacobowitz, USAF, Retired, provide a general introduction to and a commonly accepted definition of PSYOP. The authors explore the three types of PSYOP and give several examples of strategic, tactical, operational, and consolidation PSYOP. They divide propaganda into white, gray, and black classes, and present the various resources of psychological operations. The six major military objectives of PSYOP are condensed for the reader.*

ACCESSION NUMBER: ADA316643

http://handle.dtic.mil/100.2/ADA316643

Haulman, Daniel L. ***USAF Psychological Operations, 1990-2003***. Maxwell AFB, AL: Air Force Historical Research Agency, 2003. 22p.

Abstract: *Psychological operations attempt to alter the behavior of people in enemy-controlled territory. Airplanes have served as psychological instruments in recent conflicts by dropping leaflets and broadcasting radio and television messages. In conjunction with air strikes, these methods have persuaded enemy troops to surrender, abandon their positions, and stop fighting. In association with humanitarian air missions, they also have convinced civilians to turn against enemy leadership and welcome friendly forces. This paper reports on the military operations that involved psychological missions from 1990 to 2003, the advantages and disadvantages of various psychological operations, and the lessons learned from them. Only recently did the Air Force and its sister services carve out a significant place for psychological operations in their doctrine. The fact that Air Force doctrine must include psychological operations is perhaps the most important of the lessons learned since 1990. As Air Force doctrine continues to evolve, it should devote increasing attention to psychological operations. The lessons learned over the past 13 years are as follows: (1) Formulators of Air Force doctrine should continue to develop psychological operations theory; (2) Psychological operations should be part of operation plans from the beginning; (3) Psychological operations should be coordinated with other air operations; (4) Media and messages should be tailored carefully for the target population; (5) Psychological operations should complement each other; (6) Certain aircraft are more appropriate for psychological operations than others; (7) Vulnerability of psychological operations aircraft limits their use; (8) Eliminating enemy media enhances alternative information; and (9) Timing leaflet drops according to weather conditions enhances their effectiveness.*

ACCESSON NUMBER: ADA434034
http://handle.dtic.mil/100.2/ADA434034

Kerchner, Philip M., Richard F. Deckro and Jack M. Kloeber, Jr. ***Valuing Psychological Operations.*** Wright Patterson AFB, OH: Air Force Institute of Technology, 1999. 27p.

Abstract: Psychological Operations - targeting not just the physical capabilities of an opponent but the psychological dimensions as well is a key military consideration. The direct and almost instantaneous communication available with today's technology provides an even greater potential for exploiting the vulnerabilities and susceptibilities of the mind of the adversary. This effort develops a model for evaluating PSYOP products using multi-objective decision analysis and Value Focused Thinking. The model allows the Psychological Operations Detachment Commander to quantify the potential of proposed PSYOP products in meeting the psychological objectives.

ACCESSION NUMBER: ADA380231
http://handle.dtic.mil/100.2/ADA380231

Lamb, Christopher J. ***Review of Psychological Operations Lessons Learned from Recent Operational Experience***. Washington, DC: National War College, 2005. 220p.

Abstract: Extant lessons learned and guidance are correct but inadequate. Currently, psychological operations (PSYOP) are able to produce modest effects, particularly at the tactical level, with minimum resources. The Joint Staff, Joint Forces Command, and the 4th Psychological Operations Group (POG) produced joint lessons learned about PSYOP from recent operations that identify factors constraining its ability to produce greater effects. These lessons learned are accurate and consistent with the four lessons repeatedly revealed in postoperational assessments of PSYOP namely, that PSYOP performance suffers from: a lack of national-level themes to guide message formulation, slow product approval process that renders some products irrelevant, questionable product quality with uncertain effects and an overall lack of resources, including insufficient force structure.

ACCESSION NUMBER: ADA445151
http://handle.dtic.mil/100.2/ADA445151

Larsen, Stephen C. ***Conducting Psychological Operations in Sophisticated Media Environments***. Fort Leavenworth, KS: Army Command and General Staff College, June 1999. 128p.

Abstract: This study investigates doctrine, education, and training improvements necessary to produce effective Psychological Operations audio, visual, and audio-visual products in sophisticated media environments. Current ongoing operations such as that in Bosnia Herzegovina cause Psychological Operations (PSYOP) personnel affect behavioral modification in target audiences accustomed to very sophisticated media. The quality and sophistication of PSYOP products must be competitive with those other media in order to gain and hold the attention of the target audience. Recent PSYOP experience is mostly third world targeting audiences accustomed to the most basic and unsophisticated media. Current doctrine, education and training supports the conduct of PSYOP targeting audiences accustomed to relatively unsophisticated media. This thesis emphasizes proper target audience analysis and product development appropriate to sophisticated media environments. Particular attention is given to graphic design and television product development.

ACCESSION NUMBER: ADA367720
http://handle.dtic.mil/100.2/ADA367720

Lescault, Maurice A., Jr. ***The Power of Persuasion: Army PSYOP Control and Execution Entering the Third Wave***. Charlottesville, VA: Judge Advocate General's School, 1996.

Abstract: Information is creating a revolution in our society and our military. Recognizing that conflict has its root in ideology and perception affects this ideology, military units that have the capability to modulate perceptions become critical to successfully achieving national security goals. Military Psychological Operations (PSYOP) units are the only units that have this capability. Therefore, these units should be used as a true strategic asset to achieve national security objectives. To accomplish this successfully will require changes in control and execution. Enhanced control will make the routine use of military PSYOP more acceptable. Accomplishing this requires two things. First, the United States must formalize limits on the employment of PSYOP in statute and policy. Second, it must vest control of all information assets in the National Security Advisor. This consolidated control will ensure effective execution through proper integration with other activities supporting national security objectives. Efficient and effective execution will not be feasible, however, without force structure changes in military PSYOP. First, the Army should form regionalized PSYOP groups under each Regional CINC. Second, it should collocate these assets with the CINCs under their operational control. These changes in control and execution will help the United States to properly leverage information power as the Third Wave continues to change the world.

ACCESSION NUMBER: ADA438083

http://handle.dtic.mil/100.2/ADA438083

Leyda, Christopher L. ***Joint Doctrine to Integrate Theater Strategic Psychological Operations at the National Level: Searching for Needles in a Haystack.*** Newport, RI: Naval War College, 2002. 24p.

Abstract: Current joint doctrine clearly defines how a combatant commander can develop plans, organize forces, and conduct psychological operations within operational and tactical realms. However, joint doctrine stops short of providing solid mechanisms and procedures to integrate theater strategic psychological operations at the national level and with other governmental agencies responsible for information activities. A revision of joint publications: Interagency Coordination During Joint Operations (JP 3-08); Joint Information Operation (JP 3-13); and Psychological Operations (JP 3-53) must occur to clearly define a coordination mechanism to integrate theater strategic psychological operations initiatives at the national level.

ACCESSION NUMBER: ADA409154

http://handle.dtic.mil/100.2/ADA409154

Loeblein, James T. ***Building Psychological Operations (PSYOP) into the Operational Commander's Estimate of the Situation (CES).*** Newport, RI: Naval War College, 1997. 21p.

Abstract: Psychological Operations (PSYOP) provide combatant commanders with a force enhancement capability across the full military operational spectrum; from peace to crisis to war. Numerous lessons learned from the Gulf War and other recent Military Operations Other than War (MOOTW) emphasize that early, centralized planning at the highest levels form the prerequisite for effective PSYOP implementation at the Strategic, Operational, and Tactical levels of warfare. The central planning instrument for initial mission analysis and Course of Action (COA) selection is the Commander's Estimate of the Situation (CES). Presently, the Joint Operation Planning and Execution System (JOPES) broadly addresses PSYOP in both deliberate and crisis action planning. However, this doctrine fails to provide direct guidance on how to include PSYOP with all other force considerations throughout the CES. Operational planners often apply PSYOP in a shotgun approach at the end of the CES process. This application of PSYOP as a late or stand alone force or weapon system fails to incorporate the full potential PSYOP brings to the operational commander's arsenal. In contrast, PSYOP must be analyzed and compared with other force assets at the beginning of this planning process. Therefore, integrating

PSYOP directly into the CES provides the combatant commander with a well planned and synergized decision in time of peace or crisis.

ACCESSION NUMBER: ADA325152

http://handle.dtic.mil/100.2/ADA325152

Lungu, Angela M. ***WAR.COM: The Internet and Psychological Operations***. Newport, RI: Naval War College, 2001. 30p.

Abstract: As an information medium and vehicle of influence, the Internet is a powerful tool, in both open societies as well as in those whose only glimpse of the outside world is increasingly viewed and shaped through webpages, E-mail, and electronic chat rooms. Moreover, the sword cuts both ways, as unconstrained (legally, socially, politically) adversaries find the Internet an effective vehicle for influencing popular support for their cause or inciting the opposite against the U.S. or its interests. Consequently, the realm of military psychological operations (PSYOP) must be expanded to include the Internet. Just as obvious is the need for action to remove or update current policy and legal constraints on the use of the Internet by military PSYOP forces, allowing them to embrace the full range of media, so that the U.S. will not be placed at a disadvantage. Although current international law restricts many aspects of PSYOP either through ambiguity or non-currency, there is ample legal room for both the U.S. and others to conduct PSYOP using modern technology and media such as the Internet. Existing policy and legal restrictions, however, must be changed, allowing military PSYOP forces to both defend and counter adversarial disinformation and propaganda attacks which impact on the achievement of military objectives. By examining this issue, I hope to highlight the importance of the Internet for PSYOP and foment further discussion.

ACCESSION NUMBER: ADA389269

http://handle.dtic.mil/100.2/ADA389269

Mugg, David. ***Satan vs. Satan: The Use of Black PSYOP to Regain the Tactical Initiative in the Counterinsurgency Fight.*** Monterey, CA: Naval Postgraduate School, 2007. 113p.

Abstract: In the counterinsurgency fight, the insurgent has the tactical initiative because he is able to pick the time, place, and intensity of his own engagements. The insurgent s environment, however, is a very difficult one despite his initiative. The insurgent must balance the mutually exclusive requirements of hiding (operational security) and fighting (operational effectiveness) in order to gain/maintain legitimacy without being prematurely destroyed by the state. What if the state could influence this balance? What if there was a way for the state to directly target the insurgent s resource allocation between these competing requirements? Typically, states attempt this through influencing the population to support the state and reject the insurgent. But what if the state could use the insurgent s own propaganda machine against itself? Through mathematical modeling, I will show that Black PSYOP enables the state to make strategic moves on behalf of the insurgent that are so detrimental to his cause that he must act in order to counter his own moves. In this way, the state is able to turn Satan against himself. How shall then his kingdom stand? ---Matthew 12:26

ACCESSION NUMBER: ADA471500

http://handle.dtic.mil/100.2/ADA471500

http://bosun.nps.edu/uhtbin/hyperion-image.exe/07Jun%5FMugg.pdf

Muirhead, John. ***The Mind as a Target: Psychological Operations and Data Fusion Technology.*** San Antonio, TX: Air Intelligence Agency, 2001. 7p.

Abstract: Psychological Operations (PSYOP) involve actions taken to change the perceptions and ultimately the behavior of a particular foreign audience. The conduct of PSYOP requires an accurate understanding of the targeted audience and the means of influencing that audience in terms of specific goals and objectives. To accomplish this challenging category of operations directed at the minds of the target audience, PSYOP planners need access to cultural, sociopolitical, and current-event/situation data. In addition to the need for this information to be accurate, there is the critical need for the information to

be updated as close to real-time as possible. While there are initiatives underway that address these needs, a new potential may be found in the field of data fusion. The process of collection of multiple sources of data, and the correlation and combination of the data to model the target audience, is a form of data fusion. This paper introduces the discipline of PSYOP, the critical needs for data within the process of target audience analysis (TAA), and insight as to where automated data fusion processes might play a role in future PSYOP planning systems.

ACCESSION NUMBER: ADA400090

http://handle.dtic.mil/100.2/ADA400090

Mushtare, Jeremy S. ***PSYOP in Stabilization and Reconstruction Operations: Preparing for Korean Reunification.*** Monterey, CA: Naval Postgraduate School, 2005. 144p.

Abstract: Psychological operations (PSYOP) forces should undertake significant doctrinal, training, and operational reforms to ensure the viability of support provided to U.S. led stabilization and reconstruction efforts. Such operations involve increased civilmilitary interactions and necessitate effective cross-cultural communications with not only the indigenous populace, but a host of transnational actors as well. Today's PSYOP training is reflective of a persisting "Cold War mentality" that fails to adequately prepare soldiers for effective post-conflict situations such as the reunification of the Korean peninsula, whether brought about either through a renewal of combat operations or the result of diplomatic means. Meanwhile, North Korea's formidable and adept propaganda machine has persisted in isolating its populace from external influences for more than a halfcentury. Post-Korean War generation North Koreans have been successfully indoctrinated since birth to despise the United States. Furthermore, anti-U.S. sentiment has been on the rise in South Korea for a number of years. Under the current training model, contemporary psychological operations forces are ill-prepared to conduct effective operations in an environment involving two-way, face-to-face communications such as those required while stabilizing and reconstructing a nation. The case of Korean reunification serves as an extreme scenario that nevertheless depicts the drastic need for improvements in the capabilities of modern PSYOP forces.

ACCESSION NUMBER: ADA432971

http://handle.dtic.mil/100.2/ADA432971

http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Mar%5FMushtare.pdf

Perry, Kathy J. ***The Use of Psychological Operations as a Strategic Tool***. Carlisle Barracks, PA: Army War College, 2000. 26p.

Abstract: The technology revolution the world is now experiencing has changed the way we do business, the way we live, and the way we fight wars. Never before in our history has the population been exposed to the magnitude of information they are being exposed to today. This information has a direct affect on how the United States interacts with other nations, allies, and adversaries. A potential now exists to use information to our advantage in the pursuit of our national interests. This Strategic Research Paper examines the importance of using information in Psychological Operations (PSYOP) as a strategic tool for achieving national goals and objectives. It provides a review of national security policies pertaining to use of PSYOP, examines the availability and relevancy of PSYOP policy, and provides an analysis of the policy and recommendations to improve it. Additionally this research paper will analyze the use of PSYOP during Operations DESERT SHIELD and DESERT STORM (DS/DS) and examine lessons learned from the use of PSYOP as a combat multiplier during this war.

ACCESSION NUMBER: ADA377939

http://handle.dtic.mil/100.2/ADA377939

Pugmire, Brian M. ***Psychological Operations: Will the Real Approval Authority Please Stand Up?*** Newport, RI: Naval War College, 2002. 26p.

Abstract: The only organic tool the combatant commander has in his arsenal to communicate with enemy forces or civilians in his theater is Psychological Operations. Accordingly, when the Psychological Operations effort is well coordinated, it can aid significantly in the success of the commander's mission.

To be most effective Psychological Operations must be timely. Psychological Operations are most responsive when the theater level commander retains the approval authority for Psychological Operations products. The approval process begins, however, at levels well above the combatant commander. The Psychological Operations plan must be approved at the Secretary of Defense level via the Joint Staff. Considering the degree of technological advances in the information arena to which the world is now exposed, this process must have interagency coordination for a truly synchronized effort. It is imperative that during peace and war the office responsible for approving Psychological Operations plans and products be defined clearly and supported by all agencies and organizations responsible for information activities. Unfortunately, in practice, this is not always the case.

ACCESSION NUMBER: ADA401091

http://handle.dtic.mil/100.2/ADA401091

Sammons, David H., Jr. ***PSYOP and the Problem of Measures of Effectiveness (MOE) for the Combatant Commander.*** Newport, RI: Naval War College, 2004. 18p.

Abstract: *Perhaps the greatest psychological operations (PSYOP) campaign is the one in which the PSYOP community has exalted the effectiveness of their trade as a combat multiplier and peacetime contributor in the pursuit of national and military objectives. This often one-sided viewpoint dismisses the difficulty of PSYOP assessment and only exacerbates the key problem of which the total PSYOP program suffers. The Combatant Commander needs full disclosure of the facts based on the PSYOP principle of truthfulness. The reader is introduced to the doctrinal definitions of PSYOP and Measure of Effectiveness (MOE) and examples of PSYOP used in Operations ALLIED FORCE and ENDURING FREEDOM in Afghanistan. The thesis for this research paper is that PSYOP measures of effectiveness (MOE) are a significant problem that the Combatant Commander will need to address in planning and the actual conduct of war. The purpose of this paper is to assist the Combatant Commander in gaining a greater understanding of PSYOP MOE by exploring: 1) the scope of the problem, 2) the methods and procedures used to address the problem, and 3) four broad recommendations.*

ACCESSION NUMBER: ADA425993

http://handle.dtic.mil/100.2/ADA425993

Schoennauer, Eric. ***Suicide Terrorism: How Psychological Operations Can Make a Difference.*** Monterey, CA: Naval Postgraduate School, 2005. 73p.

Abstract: *Military Psychological Operations (PSYOP) is based on a Cold War construct that has not been significantly overhauled since the end of that era. Today's most pressing challenge, the Global War on Terrorism (GWOT) requires a different solution set. The Quadrennial Defense Review, the Information Operations Roadmap, the National Strategy for Combating Terrorism and the Report of the 9/11 Commission all recognize this fact. How the military PSYOP community can best adjust to this new environment and effectively address one of its major threats, that of suicide terrorism, is the subject of this paper. I will argue that examining what can, and arguably should, be done to counter the threat of suicide terrorism will also help us to see ways in which PSYOP could better be configured and employed in this new era. The first chapter of my thesis will examine the evolution of suicide terrorism in some detail but will quickly focus on what have emerged as the consensus opinions as to the motivations and vulnerabilities of this tactic. Chapter two looks at the identified motivations and vulnerabilities from a PSYOP perspective and tries to apply logical PSYOP measures against them. In chapter three I review the assets and organizational structure of the PSYOP community and suggest ways the current structure could be best applied to meet the threat. Chapter four then looks for a way ahead and focuses on how and why making three critical changes to military Psychological Operations could improve the organizations ability to accomplish its mission; not only in terms of seeking to mitigate suicide attacks but also with respect a whole host of new and expanded missions the PSYOP community will increasingly be called upon to address in the contemporary operating environment.*

ACCESSION NUMBER: ADA439671

http://handle.dtic.mil/100.2/ADA439671

http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Sep%5FSchoennauer.pdf

Siegel, Adam B. ***The Role of Civil Affairs and Psychological Operations in Humanitarian Assistance Operations.*** Alexandria, VA: Center for Naval Analyses, 1996. 44p.

Abstract: The Center for Naval Analyses (CNA) conducted a study to identify and analyze alternative ways the U.S. Marine Corps (USMC) might consider to improve its ability to conduct Humanitarian Assistance Operations (HAOs). To achieve this objective we (1) examined how the military has conducted HAOs in the past; (2) identified alternative ways the military can conduct these operations; and (3) assessed the relative costs of these alternatives in terms of changes in organization, education and training, doctrine and documentation. and equipment and supplies. The study was co-sponsored by the Marine Corps Combat Development Command (MCCDC) and I Marine Expeditionary Force (I MEF). This briefing discusses the role of Civilian Affairs (CA) and Psychological Operations (PSYOP) in HAOs, focusing on what this role means in terms of actual requirements. The briefing presents an overview of general U.S. CA and PSYOP capabilities. It discusses USMC CA and PSYOP capabilities and what theses capabilities mean for the ability of the Marine Corps to conduct operations. It also suggests ways to integrate the capabilities of the other services with Marine Corps units to more effectively conduct operations.

ACCESSION NUMBER: ADA332194

http://handle.dtic.mil/100.2/ADA332194

Sokoloski, Joseph A., III. ***Strategic PSYOP Management: A Marketing Management Approach.*** Monterey, CA: Naval Postgraduate School, 2005. 117p.

Abstract: United States Military Psychological Operations are engaged in a type of mass marketing of ideas. To accomplish this The United States Army Civil Affairs and Psychological Operations Command (USACAPOC) employs active and reserve PSYOP units to conduct PSYOP campaigns. However the methodology used to manage these campaigns often hinders the effective employment of timely and effective Psychological Operations. PSYOP has a difficult job to accomplish but PSYOP does not have the proper management tools and their national stakeholders do not understand the process. The opportunity derived from this study is to adapt principles of civilian marketing management to provide a framework and tools to develop PSYOP campaign management into a more efficient, target audience based mechanism.

ACCESSION NUMBER: ADA432676

http://handle.dtic.mil/100.2/ADA432676

http://bosun.nps.edu/uhtbin/hyperion-image.exe/05Mar%5FSokoloski.pdf

Summe, Jack N. ***Information Warfare, Psychological Operations, and a Policy for the Future***. Carlisle Barracks, PA: Army War College, March 1999. 52p.

Abstract: There is a growing interest within DoD concerning the advent of Information Warfare. This interest seems to center around two competing concepts of IW. First is the asymmetrical threat of information-based capabilities used against critical U.S. systems, and second, the burgeoning opportunities that a future Revolution in Military Affairs presents when based on the geometric growth of friendly information-based capabilities. Both analytical tracks seem to indicate that the U.S. must boldly and firmly grasp the potentialities embedded in the growing information age. Yet there are areas within the information environment that have not yet been addressed. Two such areas are a stated National policy for Information Warfare and the future strategic requirements and capabilities for the application of DoD Psychological Operations in support of our new Information Warfare policy. This paper addresses both issues and develops a point of departure for academic dialogue in these two extremely important and sensitive areas.

ACCESSION NUMBER: ADA363817

http://handle.dtic.mil/100.2/ADA363817

Thomas, Timothy L. ***New Developments in Chinese Strategic Psychological Warfare***. Fort Leavenworth, KS: Center for Army Lessons Learned, 2005. 11p.

Abstract: *Chinese military analysts have meticulously studied the use of armed force during the 1991 Gulf War and during the fight for Kosovo. They have noted with great interest the integration of military strikes and psychological-warfare activities, and the increased strategic role that the mass media played during both operations. To highlight the apparent shifting emphasis toward psychological warfare for officers of the People's Liberation Army, or PLA, the prominent Chinese military journal China Military Science has published six articles on psychological warfare during the last two years: "On PSYWAR in Recent High-Tech Local Wars," by Wang Zhenxing and Yang Suping; "The Doctrine of Psychological Operations in Ancient China," by Wu Juncang and Zhang Qiancheng; "Focus on Psychological War Against the Background of Grand Strategy," and "Psychological Operations in the Context of Grand Strategy," both written by Xu Hezhen; "Comparison of Psychological Warfare between China and the West," by Wang Lianshui, Ma Jingcheng and Yan Jianhong; and "On Defense in Modern Psychological Warfare," by Li Yuankui, Wang Yanzheng and Yang Xiaoli.*

ACCESSION NUMBER: ADA434978

http://handle.dtic.mil/100.2/ADA434978

Torres, Herminio, Jr. ***Management Meaning: The Role of Psychological Operations and Public Diplomacy in a National Information Warfare Strategy***. Monterey, CA: Naval Postgraduate School, December 1995. 59p.

Abstract: Recent advances in both the speed and breadth of communications capabilities have drastically increased the value of Strategic Political Communications. The ability of individuals to gain exposure to information beyond the control of national authorities has greatly increased the level of public engagement in foreign relations and diplomacy. However, the much discussed 'Information Revolution' is not limited to the technical advances achieved in the hardware of communications. Both Military Psychological Operations and Public Diplomacy are crucial to ensuring national strategic objectives are obtained by helping to shape international perceptions of the United States, its way of life, and its national interests. The United States needs a national level agency tasked, and granted codified authority, to devise, coordinate and implement a National Information Strategy. A National Information Strategy will bolster the National Security Strategy by focusing the efforts of all agencies involved in disseminating information for the federal government. With an understanding of the role and power of information, this agency could provide the framework for an information campaign specifically targeted to the political-military situation of an emerging crisis.

ACCESSION NUMBER: ADA306220

http://handle.dtic.mil/100.2/ADA306220

Tulak, Arthur. ***Improving Tactical Psyop Video Dissemination in Media-Austere Operating Environments***. Pearl Harbor Naval Station, HI: Pacific Command, Standing Joint Force HQ, 2004. 55p.

Abstract: U.S. video psychological operations (PSYOP) are difficult in austere operating environments lacking a mature television infrastructure. The need for video PSYOP in such environments is great, due to low literacy rates, which narrow the reach of traditional print products. Video PSYOP has generally required an extant television network and viewing audience. In operating environments where a network and viewing audience are not developed, tactical dissemination means must fill the gap. Recent operations demonstrate the requirement for video PSYOP in media-austere environments where the target audience lacks access to television, due to poverty, or lack of supporting infrastructure. Media-austere operating environments lack the indigenous TV programming necessary to attract the target audience. Accordingly, Video PSYOP also requires a supporting base of culturally appropriate video programming. PSYOP modernization efforts must obtain access to such supplemental programming while developing the technical means for tactical video dissemination. In a media austere operating environment, tailor-made video products must be created and delivered on-site, in remote villages, military bases, and cities, to small audiences using tactical dissemination systems operated by PSYOP

soldiers. Successful video PSYOP in media austere operating environments require modern, versatile tactical video dissemination means that can withstand field conditions and complement tactical operations.

ACCESSION NUMBER: ADA466225

http://handle.dtic.mil/100.2/ADA466225

Vitto, Vincent. ***The Creation and Dissemination of All Forms of Information in Support of Psychological Operations (PSYOP) in Time of Military Conflict.*** Washington, DC: Defense Science Board, 2000. 68p.

Abstract: The Terms of Reference charged the Task Force with reviewing PSYOP activities within the Department of Defense (DoD) - The purpose of the review was to: assess the capability of the United States Armed Forces to develop programming and to broadcast factual information to a large segment of the general public; assess the potential of various airborne and land-based mechanisms to deliver such information; and assess other issues in the creation and dissemination of all forms of information in times of conflict, including satellite broadcasts and the use of emerging mobile communication technologies.

ACCESSION NUMBER: ADA382535

http://handle.dtic.mil/100.2/ADA382535

Whitley, Gary L. ***PSYOP Operations in the 21st Century***. Carlisle Barracks, PA: Army War College, 2000. 38p.

Abstract: A revolution in Psychological Operations (PSYOP) will occur in the near future. The Internet will be the vehicle to enable a revolution in PSYOP and improve the capabilities of PSYOP to achieve objectives specified in the National Security Strategy (NSS). The paper is structured to support this thesis by first providing a detailed definition and description of PSYOP. Next the importance of communication techniques in developing PSYOP methods is described. The understanding gained from these sections is then used to emphasize how the Internet can revolutionize PSYOP. Reflex control was presented as a method of PSYOP for the future. Then, based on the knowledge presented in this paper, some recommendations are made on how the Internet could be used to revolutionize future PSYOP campaigns. PSYOP has been an essential element of warfare since ancient times. PSYOP will continue to be a key strategic weapon to provide the ways to accomplish the objectives specified in the NSS. As Napolean Bonaparte once said, "There are but two powers in the world, the sword and the mind. In the long run the sword is always beaten by the mind".

ACCESSION NUMBER: ADA378002

http://handle.dtic.mil/100.2/ADA378002

Legal Aspects

Books

Aldrich, Richard W. **The International Legal Implications of Information Warfare**. [Colorado Springs], CO: USAF Institute for National Security Studies, 1996. 33p.
http://www.usafa.af.mil/df/inss/OCP/ocp9.pdf
DKL D 305.24:9 FEDDOCS

Greenberg, Lawrence T. and Kevin J. Soo Hoo. **Old Law for a New World?: Applicability of International Law to Information Warfare**. Stanford, CA: Stanford University, Institute for International Studies, Center for International Security and Arms Control, 1997. 38p.

Greenberg, Lawrence T., et al. **Information Warfare and International Law.** Washington, DC: National Defense University, [1998]. 53p.
http://www.dodccrp.org/files/Greenberg_Law.pdf
DKL KZ6718 .G74 1997 GENERAL

Miller, Robert D. **International Law: How it Affects Rules of Engagement and Responses in Information Warfare?** Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 40p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1037

O'Brien, Gregory John. **The International Legal Limitations on Information Warfare.** Thesis (LL.M.)--George Washington University, 1998. 83p.
DKL JX1295 .O274 1998 GENERAL

Shawhan, Karl J. **Vital Interests, Virtual Threats: Reconciling International Law with Information Warfare and United States Security.** Maxwell Air Force Base, AL: Air University Press, [2001]. 57p.
http://aupress.maxwell.af.mil/SAAS_Theses/SAASS_Out/Shawhan/shawhan.pdf
DKL D 301.26/6:I 54 FEDDOCS

Shulman, Mark R. **Legal Constraints on Information Warfare**. Maxwell Air Force Base, AL: Air University, Center for Strategy and Technology, Air War College, 1999. 34p. *http://www.au.af.mil/au/awc/awcgate/cst/csat7.pdf* *OR*
http://handle.dtic.mil/100.2/ADA407469
DKL D 301.26/6-A:7 FEDDOCS

Vadnais, Daniel M. **Law of Armed Conflict and Information Warfare--How Does the Rule Regarding Reprisals Apply to an Information Warfare Attack?** Maxwell AFB, AL: Air University, Air Command and Staff College, 1997. 27p.
https://research.maxwell.af.mil/viewabstract.aspx?id=1010

United States. Department of the Air Force. **A Primer on Legal Issues in Information Warfare**. Washington, DC: HQ USAF/JAI, 1995. 27p.

Periodicals

Aldrich, Richard W. "The International Legal Implications of Information Warfare." **Airpower Journal**, Fall 1996, v. 10, no. 3, p. 99-110. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/fall96/aldricha.html* OR *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/fall96/aldrich.pdf*

Anthes, Gary H. "New Laws Sought for Info Warfare." **Computerworld**, June 5, 1995, v. 29, no. 23, p. 55.

Broucek, Vlasti and Paul Turner. "Intrusion Detection: Issues and Challenges in Evidence Acquisition." **International Review of Law, Computers & Technology**, July 2004, v. 18, no. 2, p. 149-164.

Chaisson, Kernan. "Cyber Warfare Rules "Bumfuzzle" DoD Lawyers." **Journal of Electronic Defense**, January 2000, v. 23, no. 1, p. 16-17.

Delibasis, Dimitrios. "The Right of States to Use Force in Cyberspace: Defining the Rules of Engagement." **Information and Communications Technology Law**, October 2002, v. 11, no. 3, p. 255-268.

Dhillon, Joginder S. and Robert I. Smith. "Defensive Information Operations and Domestic Law: Limitations on Government." **Air Force Law Review**, 2001, v. 50, p. 135-174.

DiCenso, David J. "Information Operations: An Act of War?" **Law Technology**, 2nd Quarter 2000, v. 33, no. 2, p. 26-44.

_____. "IW (Information Warfare) Cyberlaw: The Legal Issues of Information Warfare." **Airpower Journal**, Summer 1999, v. 13, no. 2, p. 85-102; **Law/Technology**, 2nd Quarter 2000, v. 33, no. 2, p. 1-25. *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/sum99/dicenso.html* OR *http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/sum99/dicenso.pdf*

Goldberg, Michael B. "The Legal Implications on Information Operations." **Cyber Sword**, Fall 1999, v. 3, no. 1, p. 23-25.

Grove, Gregory D., Seymour E. Goodman and Stephen J. Lukasik. "Cyber Attacks and International Law." **Survival**, November 2000, v. 42, no. 3, p. 89-103.

Hanseman, Robert G. "The Realities and Legalities of Information Warfare." **Air Force Law Review**, 1997, v. 42, p. 173-200.

Haslam, Emily. "Information Warfare: Technological Changes and International Law." **Journal of Conflict and Security Law**, 2000, v. 5, no. 2, p. 157-175.

Hunter, Garry E. “The Use of Technology to Invade Personal Privacy in the Interest of Collective Security: Does the End Justify the Means?” **Law Technology**, 1st Quarter 2007, v. 40, no. 1, p. 1-20.

Jacobson, Mark R. “War in the Information Age: International Law, Self-Defense, and the Problem of 'Non-Armed' Attacks.” **Journal of Strategic Studies**, September 1998, v. 21, no, 3, p. 1-23.

Johnson, David R. and David Post. “Law and Borders – the Rise of Law in Cyberspace.” **Stanford Law Review**, May 1996, v. 48, no. 5, p. 1376-1402.

Johnson, R. A. “Justification for an Active Defense Against a Computer Attack Under International Law.” **Cyber Sword**, Spring 2000, v. 4, no. 1, p. 24-26.

Joyner, Christopher C. and Catherine Lotriontе. “Information Warfare as International Coercion: Elements of a Legal Framework.” **European Journal of International Law**, December 2001, v. 12, no. 5, p. 825-865.

Kanuck, Sean P. “Information Warfare: New Challenges for Public International Law.” **Harvard International Law Journal**, Winter 1996, v. 37, no. 1, p. 272-292.

Lessig, Lawrence. “The Path of Cyberlaw.” **Yale Law Review**, May 1995, v. 104, no. 7, p. 1743-1755.

Macklin, James. “Information Operations and the Law: A Practical Guide for Signal Planners and Operators.” **Army Communicator**, Fall 1999, v. 24, no. 3, p. 12-16.

Morth, Todd A. “Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2 (4) of the U.C. Charter.” **Case Western Reserve Journal of International Law**, Spring/Summer 1998, v.30, no. 2/3, p. 567-600.

“Network Defense Hinges on Standards, Legal Reform.” **Signal**, March 2000, v. 54, no. 7, p. 26.

Schmitt, Michael N. “Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict.” **Michigan Journal of International Law**, Summer 1998, v. 19, no. 4, p. 1051-1090.

Schmitt, Michael N. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.” **Columbia Journal of Transnational Law**, 1999, v. 37, no. 3, p. 885-938.

Schmitt, Michael N. “The Principle of Discrimination in 21st Century Warfare.” **Yale Human Rights and Development Law Journal**, 1999, v. 2, p. 143-182.

Scott, Roger D. “Legal Aspects of Information Warfare: Military Disruption of Telecommunications.” **Naval Law Review**, 1998, v. 45, p. 57-76.

Shulman, Mark R. “Discrimination in the Laws of Information Warfare.” **Columbia Journal of Transnational Law**, 1999, v. 37, no. 3, p. 939-968.

Smyczek, Peter J. “Regulating the Battlefield of the Future: The Legal Limitations on the Conduct of Psychological Operations (PSYOPS) Under Public International Law.” **Air Force Law Review**, 2005, v. 57, no. 209-240.

Stahl, Pamela M. and Toby Harryman. “Center for Law and Military Operations (CLAMO) Report.” **The Army Lawyer**, March 2004, p. 30-38.

Terry, James P. “Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What at the Targeting Constraints?” **Military Law Review**, September 2001, v. 169, no. 1, p. 70-91.

Warren, Matthew and William Hutchinson. “The Law and Cyber Terrorism.” **Journal of Information Warfare**, March 2003, v. 2, no. 2, p. 27-32.

Wingfield, Thomas C. "Legal Aspects of Offensive Information Operations in Space." **Journal of Legal Studies [USAFA]**, 1998/1999, v. 9, p. 121-146.

Documents, Theses & Technical Reports

Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography.

Aldrich, Richard W. ***Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime.*** US Air Force Academy, CO: Institute for National Security Studies, 2000. 104p.

Abstract: This is the 32nd volume in the Occasional Paper series of the U.S. Air Force Institute for National Security Studies (INSS). This paper, along with Occasional Paper 33, Steven Rinaldi's "Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security," address the context surrounding the question of how the U.S. military responds to the cyber threat facing the American military and society today. Rinaldi examines the issues of partnering and sharing sensitive information across private and governmental sectors as a central requirement of a national risk reduction and management effort in the face of the threat of cyber attack. In this paper, Richard Aldrich examines definitional and jurisdictional issues, constitutional and statutory concerns, and both the necessity and desirability of an international treaty addressing cyberterrorism and computer crime. Together these two papers provide fresh thinking and critical perspective on a security threat arena that increasingly captivates the headlines.

ACCESSION NUMBER: ADA435088

http://handle.dtic.mil/100.2/ADA435088

Bond, James N. ***Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)***. Newport, RI: Naval War College, June 1996. 110p.

Abstract: The report discusses the issue of whether manipulation of a foreign state's data may be considered to be the use of force against that country in violation of Article 2(4) of the U.N. Charter. The paper first reviews the different methods of interpreting treaties such as the U.N. Charter, then examines briefly whether Article 2(4) is still a valid norm under international law. The paper concludes that in certain circumstances data manipulation could be the use of force, but is more likely to be considered an intervention in the internal affairs of the foreign state than the use of force.

ACCESSION NUMBER: ADA310926

http://handle.dtic.mil/100.2/ADA310926

Ellis, Bryan W. ***The International Legal Implications and Limitations of Information Warfare: What Are Our Options?*** Carlisle Barracks, PA: Army War College, 2001. 29p.

Abstract: When we examine the relationship between information warfare (IW) and the law, particularly international law and the law of war, it becomes apparent that fundamental questions need to be explored. How is "war defined as it relates to IW and what activities will we define as IW? Who are considered combatants in IW? How do the terms "force, "armed attack," or "aggression" equate or relate to IW? Does "war require physical violence and human casualties? How will established legal principles related to national sovereignty be affected by IW? These questions and issues merely hint at the tremendous uncertainties surrounding the evolving discipline of IW. This paper examines IW from a layman's legal perspective and explores issues such as the law of war and standing international agreements to which the United States is a signatory. The concept for the employment of IW is evolving and as recently demonstrated in Yugoslavia, legal constraints, limitations, and issues appear to be the norm. There is currently no authoritative legal or international agreement as to whether an IW "attack" is

comparable to an "attack" or "use of force" in the traditional sense. With this as a context, the study identifies several legal approaches our armed forces could employ offensively, defensively, or in retaliation to an information attack.

ACCESSION NUMBER: ADA389043

http://handle.dtic.mil/100.2/ADA389043

Haber, Matthew E. ***Computer Network Attack and the Laws of Armed Conflict: Searching for Moral Beacons in Twenty-First-Century Cyberwarfare.*** Fort Leavenworth, KS: Army Command and Staff College, 2002. 123p.

Abstract: *Computer network attack ushered in change for the profession of arms. Militaries achieve effects using computers, previously attained only through physical destruction. Computer network attack's problem is it operates outside the observable domain the laws of armed conflict describe, yet its effects are what the laws address. Thus, the primary research question is: Does a legal framework of analysis exist for computer network attack? The secondary question became: If a framework exists, is it applied consistently throughout the Department of Defense? A search of literature and interviews with information operators and their associated lawyers revealed a framework by Thomas Wingfield. The framework analyzes the level of force but does not address the four basic principles for warfare; military necessity, humanity, proportionality, and discrimination. Also, the framework is not applied throughout the Department of Defense. The Joint Task Force Computer Network Operations' creation is the first step in building a hierarchical structure for consistent application of law to computer network attack. Research recommends such a structure expand Wingfield's framework for computer network attack to be a viable weapon for Twenty-First-Century Warfare.*

ACCESSION NUMBER: ADA406496

http://handle.dtic.mil/100.2/ADA406496

Henseler, Sean P. ***Addressing the Legal Challenges of Network Centric Warfare. Case In Point: The Legal Implications of Obtaining an "Information and Knowledge Advantage" Prior to Hostilities.*** Newport, RI: Naval War College, 2001. 28p.

Abstract: *If it is true that the Navy is moving away from platform-centric toward network-centric warfare (NCW), then its leaders must ensure that any such transition is accomplished in the most efficient and effective manner possible. Since the Navy's current vision of net-centric operations raises many complex and often unsettled legal issues, the Navy must establish a formal framework for analyzing the legal challenges posed by NCW then integrate this framework into any NCW transition process. Future net-centric operational commanders have a vested interest in ensuring that the legal implications of NCW on factor space, time, and forces have been thoroughly considered. Current and future international and domestic law might limit the ability of net-centric commanders to optimize the key concepts of the Navy's vision of net-centric operations. If the technological and doctrinal aspects of NCW continue to rapidly evolve without regard for the legal challenges, the Navy might find itself in a position where it has invested a tremendous amount of time and money developing a system of sensors and platforms that cannot be employed as envisioned due to legal constraints.*

ACCESSION NUMBER: ADA389546

http://handle.dtic.mil/100.2/ADA389546

Information Warfare**: **Legal**, **Regulatory, Policy and Organizational Considerations for Assurance. McLean VA: Science Applications International Corporation, 1995. 454p.

Abstract: *Performing essential national security-related functional activities is depending more and more on a rapidly evolving, supporting information infrastructure. In view of the dependency, and because the Department of Defense (DoD) information infrastructure is embedded in larger national and international infrastructures, DoD officials, their advisors, and others within and outside the government have recommended to the National Security Council staff that it may be necessary to initiate*

interdepartmental/interagency discussions. Topics of such a dialogue would include the dependency and vulnerability issues and the need for national policy to deal with them. The Chief, Information Warfare Division (J6K), Directorate of Command, Control, Communications, and Computer Systems (J6), the Joint Staff, commissioned this report to prepare the Joint Staff to participate in and contribute to these discussions. The breadth and extreme complexity of the subject matter, other related ongoing activities, and the scope of the task limited the number of environmental areas and organizations which could be addressed. The report does, however, address the breadth and complexity of the policy and strategy issues and summarize the views of those in positions of importance to the development of policy for information warfare. To develop the organizational policy considerations, the study group reviewed organizations which have a stated role in information warfare and organizations which have related missions and functions. This report presents several key organizations in a broad range encompassing international, national, state and local, public and private, government and industry organizations. The environmental areas examined were: Information Infrastructure, Legal Environment, Regulatory Environment, Policy Environment, Emerging Technologies, Adversary Capabilities.

ACCESSION NUMBER: ADA316285

http://handle.dtic.mil/100.2/ADA316285

Kuschner, Karl W. ***Legal and Practical Constraints on Information Warfare***. Newport, RI: Naval War College, June 1996. 22p.

Abstract: Information warfare weapons must meet the same tests for necessity and proportionality as other weapons under the laws of armed conflict. In addition, commanders must recognize and weigh the possible consequences of weapons that can devastate the information systems of an adversary. Problems such as lack of enemy command and control, post-hostility reconstruction, and retaliation, among others, must be considered by the commander contemplating the use of information weapons.

ACCESSION NUMBER: ADA307433

http://handle.dtic.mil/100.2/ADA307433

Lipinski, T. A. “Information Warfare American Style: The Battle for Page Numbers, Real Time Event Data and Other Factual Information. Recent Legal Developments.” P. 105-115, IN: ***Technology and Society, 1998. ISTAS 98. Wiring the World: The Impact of Information Technology on Society***. Proceedings of the 1998 International Symposium, June 12-13 1998. 176p.

Abstract: The development of the National Information Infrastructure opens new avenues for information products and services. As these information products and services are developed and marketed, the producers of those products and service seek to protect their proprietary interest in the underlying information. Attempts to extend legal protection to basic facts and other public domain information demonstrate that the public information space is eroding. Recent information controversies can form the basis for establishing several predictors useful in determining when future information ownership controversies may develop and result in the loss of public information space. One set of predictors describes the information environment. A second set of predictors characterizes the marketplace environment. Identifying instances where elements of each set of predictors exist suggest a change in information rights or ownership most likely to result in the critical loss of access to public information space.

Meader, Gerald H. ***Information Warfare: Few Challenges for Public International Law***. Wright-Patterson AFB, OH: Air Force Institute of Technology, September 1997. 56p.

Abstract: Information Warfare is of Rising Concern A threshold question is, Why address this issue at all. It deserves a look because our increasing dependence on information and information technologies makes us ever more vulnerable to this attractive, elegant weapon. Dependence on the National Information Infrastructure According to a recent report by a Defense Science Board Task Force, the information infrastructure of the United States is increasingly vulnerable. Indeed, because the U.S. is so

very dependent on information technology, it is one of the most vulnerable nations to IW attack. This vulnerability extends to infrastructures related to military C4I, oil and gas control, water supply, government operations, mass media, civil emergency services, transportation control, finances (national and global), and production, inventory and process controls. They are vulnerable because all of these systems use increasingly complex, interconnected network control systems. These infrastructures are also interdependent such that an attack on one could have a cascade effect on others.

ACCESSION NUMBER: ADA329719

http://handle.dtic.mil/100.2/ADA329719

Miller, Earl E. ***Army Transformation and Information Operations: The International Legal Implications.*** Carlisle Barracks, PA: Army War College, 2002. 35p.

Abstract: *As many nations throughout the world have become entrenched in what has been described as the information revolution, many legal parameters of information operations remain uncertain. Information is fast becoming a strategic resource that permeates every facet of the U.S. National Military Strategy. The proliferation of information-based technologies will substantially transform the Army's doctrine as well as its structure. The evolution of the information environment has specific legal implications within the international community. This paper examines these challenges and proposes to establish a framework for the inevitable global debate over related legal issues.*

ACCESSION NUMBER: ADA404415

http://handle.dtic.mil/100.2/ADA404415

Miller, Robert D. ***International Law: How It Affects Rules of Engagement and Responses in Information Warfare.*** Maxwell Air Force Base, AL: Air University, 1997. 48p.

Abstract: The importance of reliable, timely information to the success of military operations, while precluding an adversary from accessing information, has been known since wars began. Today, a combination of electronic devices, such as computers and sensors, are creating an "information age" that redefines how we conduct military operations. A major challenge to decision makers and military leaders is to understand the impact of international laws in the information age and its influence on rules of engagement (ROE), and response development. By all accounts, our dependence on information and information systems will continue to grow along with technological advances, enhancing our own command, control, communications, computer, and information capabilities, while also increasing our vulnerabilities. As a result, a key issue our decision makers and military leaders must be aware of concerns the legal considerations in using IW and in responding to IW threats and attacks. Developers of our ROE must provide the guidance for legally, appropriately responding to IW attacks, while ensuring the right to self-defense. Our leaders must also devise appropriate response options against foreign powers conducting IW operations against the US. We must base responses on the level of threat to our national interests, while considering intent, international law, and elements such as proportionality and necessity inherent in the Law of Armed Conflict.

ACCESSION NUMBER: ADA394055

http://handle.dtic.mil/100.2/ADA394055

O'Brien, Gregory J. ***International Legal Limitations on Information Warfare***. Washington, DC: George Washington University, School of Law, May 1998. 85p.

Abstract: We live in an age that is driven by information. Technological breakthroughs... are changing the face of war and how we prepare for war. Information war has no front line. Potential battlefields are anywhere networked systems allow access to oil and as pipelines, for example, electric power grids, telephone switching networks. In sum, the U.S. homeland may no longer provide a sanctuary from outside attack. A panel of Defense Department experts recently warned the nation about the prospect of an electronic Pearl Harbor, a crippling sneak attack on the nation's defense and civilian information systems in which 'cyberterrorists' and other unknown assailants cripple the nation's, or the world's, computer-networked communications, financial, and national defense systems.

ACCESSION NUMBER: ADA365127
http://handle.dtic.mil/100.2/ADA365127

Pottorff, James P., Jr. ***Legal Preparation of the Battlefield: Issues in Combined Operations***. Newport, RI: Naval War College, May 1999. 25p.
Abstract: This JMO paper discusses the issues arising when allies and coalition partners in combined operations have different laws and policies with regard to such matters as antipersonnel land mines, rules of engagement, and protected places. Recognition, analysis, and, when possible, reconciliation of domestic law and policy differences among members of a coalition or alliance should be included in a CINC's planning for any combined operation. In that light, this paper discusses the implications of differences in law and policy among members of multinational forces, highlights several of the more significant of these issues, and proposes some solutions that may mitigate, if not alleviate, problems created by these variations..
ACCESSION NUMBER: ADA370645
http://handle.dtic.mil/100.2/ADA370645

Roig, William A. ***Creating Rules of Engagement for Information Warfare: Examining the Policy Implications of International Law***. Newport, RI: Naval War College, Joint Military Operations Department, June 1997. 20p.
Abstract: Achieving the full revolutionary impact of information warfare requires distinguishing the methods of information attack from other forms of warfare on policy and legal grounds. Information attack represents a revolutionary new form of warfare from a legal perspective because it allows a severe effect, and therefore intense coercion, to occur with little or no violence and little traditional destruction.
ACCESSION NUMBER: ADA328161
http://handle.dtic.mil/100.2/ADA328161

Smits, Theodore V. ***Computer Network Attack as a Tool for the Operational Commander.*** Newport, RI: Naval War College, Joint Military Operations Department, 2000. 28p.
Abstract: Computer network attack provides the capability for an attack to be carried out at the speed of light, effortlessly across international boundaries. It has the potential to provide the Operational Commander additional capabilities along the entire spectrum of warfare from deterrence to combat operations. Key enemy systems, including radar, air traffic control and communications have the potential to be rapidly removed from operation without having to move a single plane, put U.S. personnel in harms way or expend expensive precision guided munitions. However, the law of armed conflict and other international laws raise legal issues that potentially limit the implementation of this new weapon. The Operational Commander must be knowledgeable of the basis of the legal issues so that suitable network attack targets can be selected during the operational plan development, targets against which an attack plan can be developed and approved in the period required to support the attack's employment in the conflict.
ACCESSION NUMBER: ADA378752
http://handle.dtic.mil/100.2/ADA378752

Vadnais, Daniel M. ***Law of Armed Conflict and Information Warfare--How Does the Rule Regarding Reprisals Apply to an Information Warfare Attack?*** Maxwell AFB, AL: Air Command and Staff College, 1997 34p.
Abstract: The question of how to characterize an information warfare attack, particularly what is known as a "hacker attack,: has not been fully developed. It must be, though, in order to understand how a nation can respond to it. This paper explores applicable tenets of international law. It identifies various methods of engaging in the spectrum of activities known as information warfare, and then discusses the

one that has been underexplored in the context of a military response. Finally, it addresses the applicability of the law of armed conflict to a "hacker attack." Given that during wartime, almost any means of imposing one belligerent's will on another is legitimate, subject to the various tenets international law, the question that needs to be addressed is what range of activities is permissible during times other than war, when parties are not engaged in traditionally understood applications of armed force." The current body of international law seems to mitigate against including hacking" in the definition of armed force," the standard necessary for unilateral military armed reprisal actions. In that case, unless the initial attack rises to the level that would permit some action by the "victim" in self-defense, that nation is relegated to seeking action from the United Nations Security Council.

ACCESSION NUMBER: ADA392890

http://handle.dtic.mil/100.2/ADA392890

Washington, Ollie, Jr. ***The Legal and Ethical Implications of Information Operations***. Carlisle Barracks, PA: Army War College, 2001. 29p.

Abstract: *Information Operations (I0) is a family of programs and tools that are used to deprive or disrupt an adversary's information and information systems while assuring the continued availability of your own. The technological tools of IO have been developed and implemented so rapidly that the domestic and international laws that should govern their use have not kept pace. Hackers, cyber criminals, terrorist and foreign spies are using tools such as computer network attack while domestic and international laws are insufficient to adequately patrol them. Further, there are ethical issues involved in the use of these IO tools that may not have been adequately debated, at least from a societal standpoint, to mediate possible conflicts with our national values. IO tools will allow the U.S. to engage and disable enemy facilities previously engaged with kinetic weapons, without the physical collateral damage, but with possible significant impact on noncombatants. International agreements such as the Geneva Convention do not specifically address IO and even within the U.S. military the rules of engagement on IO are not clear. This paper will attempt to explore some of these incongruities and provide a perspective on where the U.S. stance could be on our use of IO.*

ACCESSION NUMBER: ADA390619

http://handle.dtic.mil/100.2/ADA390619

Wingfield, Thomas C. ***Legal Aspects of Offensive Information Operations in Space***. Washington, DC: Department of Defense, 2005. 17p.

Abstract: *What, then, are the specific steps to follow in performing a legal analysis of offensive information operations in space? First, correctly identify the type and subtype of operation contemplated. The three types are intelligence collection, offensive operations through satellites, and offensive operations against satellites. The subtypes for each are listed in the second section of this paper. Second, determine if this type of operation, in the light of all relevant circumstances, rises to the level of a use of force. Although international legal academics are only now turning to this question, the one settled concept in this area is that an information operation crosses the Article 2(4) threshold when it produces effects comparable to those of a kinetic attack which would be thought of as having crossed the threshold. What more than that would constitute a use of force is still an open question. If the action is the equivalent of a use of force, it may only be undertaken pursuant to Chapter VII authorization, or as a lawful exercise of self-defense. Assuming the legality of acting at all, the operation must be conducted in accordance with the customary international legal standards of proportionality, discrimination, and chivalry. Offensive information operations in space will drive a revolution in technical, tactical, and legal thought. It is for the attorney adviser to the warfighter to present honest, closely reasoned legal advice to his client so that he may fight honorably and effectively.*

ACCESSION NUMBER: ADA435835

http://handle.dtic.mil/100.2/ADA435835

Zengel, Patricia. ***Responding with Force to Information Warfare: Legal Perspectives***. Newport, RI: Naval War College, May 1996. 25p.

Abstract: The advent of Information Warfare (IW), heralded by many as an approaching Revolution in Military Affairs (RMA), has raised questions concerning the ability of the existing body of international law to respond to novel legal issues that IW will inevitably pose, specifically with regard to the use of force to counter IW attack. It has been suggested that a new or significantly expanded body of international law might be required to address issues pertaining to the use of force in the context of IW. Upon closer examination, however, it appears that while existing law in this area does not necessarily provide definitive and universally accepted answers to all questions that may arise, it does provide the needed structure for analysis. The development of international law in this area will be evolutionary rather than revolutionary.

ACCESSION NUMBER: ADA312081

http://handle.dtic.mil/100.2/ADA312081

Doctrine Publications

Joint Publications

Joint Pub 3-13 -- **Joint Doctrine for Information Operations**
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

Joint Pub 3-13.1 -- **Joint Doctrine for Command and Control Warfare (C2W)**
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_1.pdf

Joint Pub 3-53 -- **Doctrine for Joint Psychological Operations**
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_53.pdf

Joint Pub 3-58 – **Joint Doctrine for Military Deception**
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_58.pdf

US Air Force Doctrine pubs

AFDD 2-5 **Information Operations**
http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5.pdf

AFDD 2-5.1 **Electronic Warfare Operations**
http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5_1.pdf

AFDD 2-5.3 **Public Affairs Operations**
http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_5_3.pdf

US Army Doctrine Pubs

FM 3-05.30 **Psychological Operations**
http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

FM 3-05.301 (MCRP 3-40.6A) **Psychological Operations Tactics, Techniques, and Procedures**
http://www.fas.org/irp/doddir/army/fm3-05-301.pdf

FM 3-05.302 **Tactical Psychological Operations: Tactics, Techniques, and Procedures**
http://www.fas.org/irp/doddir/army/fm3-05-302.pdf

FM 100-6 **Information Operations**
http://www.fas.org/irp/doddir/army/fm100-6/

US Marine Corps Doctrine Pubs

MCDP 6 **Command and Control**
http://www.dtic.mil/doctrine/jel/service_pubs/mcdp6.pdf

US Navy Doctrine Pubs

NDP 6 **Command and Control**
http://www.dtic.mil/doctrine/jel/service_pubs/ndp6.pdf

Directives and Instructions

OPNAVINST 3430.25 **Information Warfare and Command and Control**
http://neds.daps.dla.mil/Directives/3430_25.pdf

OPNAVINST 3430.26 **Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W)**
http://neds.daps.dla.mil/Directives/3430_26.pdf

OPNAVINST 3434.1 **Psychological Operations**
http://neds.daps.dla.mil/Directives/3434_1.pdf

PDD 63 [Presidential Decision Directive] -- **Protecting America's Critical Infrastructures**
http://www.fas.org/irp/offdocs/pdd-63.htm
and White Paper -- *http://www.fas.org/irp/offdocs/paper598.htm*

Bibliographies

"An IW Bibliography."
http://all.net/books/iw/iwarstuff/www.infowar.com/resource/iwbib1.html

Alexander, Debra. **Information Operations**. Maxwell AFB, AL: Air University Library, 2006. http://www.au.af.mil/au/aul/bibs/informops.htm

Armstrong, Glenda. **Information Operations: AFSC Research Topic**. Maxwell Air Force Base, AL: Air University Library, 2005. *http://www.au.af.mil/au/aul/bibs/io/io5.htm*

Chun, Stephen. **Information Warfare** -- SOS Current Military Issues Topic, Maxwell AFB, AL: Air University Library. *http://www.au.af.mil/au/aul/bibs/infowar/if.htm*

Donnelly, Barbara R. "Deception." **Naval War College Library Notes**, November 2002, v. 31, no. 3.
http://www.nwc.navy.mil/library/3Publications/NWCLibraryPublications/LibNotes/libdeception.htm

Ottaviano, Doris B. **Network Centric Warfare: An Update**. Newport, RI: Naval War College Library, July 2001.
http://www.nwc.navy.mil/library/3Publications/NWCLibraryPublications/LibNotes/libnetwork.htm

Ottaviano, Doris B. **Network Centric Warfare: A 2002 Update**. Newport, RI: Naval War College Library, 2002.
http://www.nwc.navy.mil/library/3Publications/NWCLibraryPublications/LibNotes/bibNetCentricWar2002.htm

Pastorett, Tomma N. **Information Warfare: Selected References**. Maxwell Air Force Base, AL: Air University Library, 1996. http://www.au.af.mil/au/aul/bibs/infowar/infor.htm

Rauch, Marguerite C. "Information Warfare." **Naval War College Library Notes**, December 1995, v. 24, no. 1.
http://www.nwc.navy.mil/library/3Publications/NWCLibraryPublications/LibNotes/libinfwf.htm

Rowe, Cathy E. "Information Warfare Update." **Naval War College Library Notes**, October 1998, v. 27, no. 3,.
http://www.nwc.navy.mil/library/3Publications/NWCLibraryPublications/LibNotes/libinfwf-update.htm

Rowe, Wayne J. "Network Centric Warfare," **Naval War College Library Notes**, May 1999, v. 27, no. 4.
http://www.nwc.navy.mil/library/3Publications/NWCLibraryPublications/LibNotes/libnetwork.htm

Sanz, Timothy L. “Information-Age Warfare: A Working Bibliography, pt 2.” **Military Review**, September-November 1998, v. 78, no. 5, p. 41-50. Pt 1, v. 78, no. 2 (March-April 1998), p. 83-90.

Seymore, Janet. **Deception in Warfare.** Maxwell AFB, AL: Air University Library, 1996.
http://www.au.af.mil/au/aul/bibs/decwar/dwtoc.htm

Shope, Virginia C. **Information: A Selected Bibliography**. Carlisle Barracks, PA: US Army War College library, 1998.
http://carlisle-www.army.mil/library/bibs/infowar.htm

Internet Sites

Command and Control Research Program (CCRP) -- *http://www.dodccrp.org/*
C2 Bibliography -- *http://www.dodccrp.org/html4/research_c2.html*
C2 Journal -- *http://www.dodccrp.org/html4/journal_main.html*
Information Superiority -- *http://www.dodccrp.org/html2/research_other.html*
Network Centric Warfare -- *http://www.dodccrp.org/html4/research_ncw.html*

Center for Information Systems Security Studies and Research (CISR) [NPS]
http://cisr.nps.navy.mil/
Publications -- *http://cisr.nps.navy.mil/pub_papers.html*

CyberSecurity Intelligence Threat Assessments (Federation of American Scientists)
http://www.fas.org/irp/threat/cyber/

Cyberspace & Information Operations Study Center
http://www.au.af.mil/info-ops/law.htm

Information Assurance Technology Analysis Center [IATAC]
http://iac.dtic.mil/iatac/

Information Warfare and Information Security on the Web [American Federation of Scientists] -- *http://www.fas.org/irp/wwwinfo.html*

InfoSec and InfoWar Portal -- *http://www.infowar.com/*

Institute for the Advanced Study of Information Warfare [IASIW] --
http://psycom.net/iwar.1.html

IWS – Information Warfare Site
http://www.iwar.org.uk/

Navy Information Operations Command Norfolk
https://www.nioc-norfolk.navy.mil/