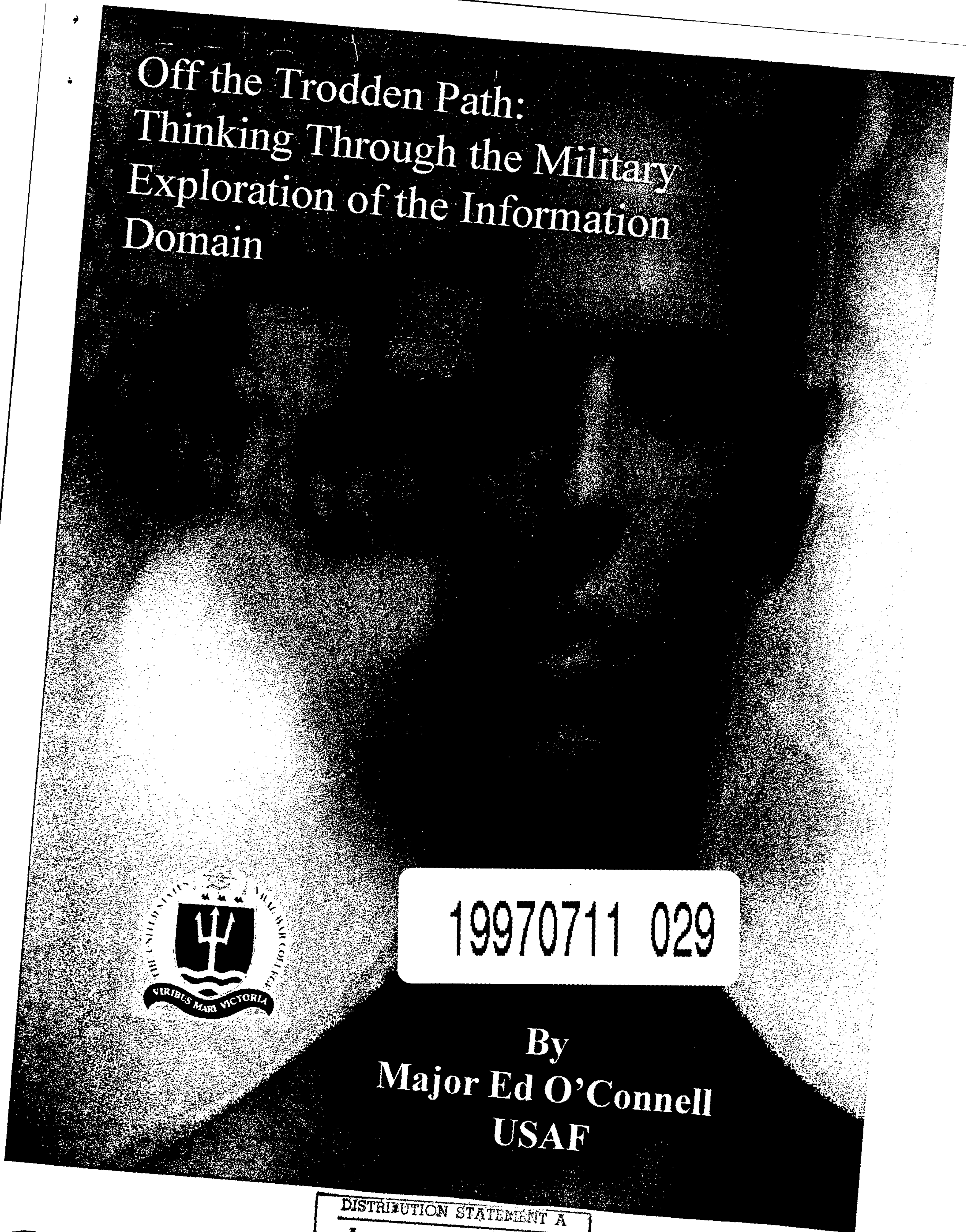
Off the Trodden Path: Thinking Through the Military Exploration of the Information Domain



19970711 029

By
Major Ed O'Connell
USAF

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS N/A
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT UNLIMITED
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION / 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code)	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION Advanced Research Dept 8b. OFFICE SYMBOL (If applicable) 35	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code) Naval War College 686 Cushing Rd Newport, RI 02841-1207	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification) Off the Trodden Path: Thinking Through the Military Exploration of the Information Domain

12. PERSONAL AUTHOR(S) MAJor Ed O'Connell, USAF

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Final	FROM Nov 96 TO Feb 97	21 Feb 1997	85

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Information warfare, cyberspace, national security interests

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

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.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL CDR Joe Vanderlip, Asst. ARP	22b. TELEPHONE (Include Area Code) 401-841-6568	22c. OFFICE SYMBOL 35A

DD FORM 1473, 84 MAR

83 APR edition may be used until exhausted.
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

☆U.S. Government Printing Office: 1985—539-012

0102-LF-014-6602

NAVAL WAR COLLEGE
Newport, R.I.

Off the Trodden Path: Thinking Through the Military Exploration of the Information Domain

by

Edward P. O'Connell

Major, United States Air Force

As an Advanced Research Project

A paper submitted to the director of the Advanced Research Department in the Center for Naval Warfare Studies in partial satisfaction of the requirements for the Masters of Arts Degree in National Security and Strategic Studies.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: Edward P. O'Connell

21 February 1997

Paper directed by John B. Hattendorf, Ph.D.
Director, Advanced Research Department

____________________ ________
(Faculty Advisor) (Date)
Roger W. Barnett, Ph.D.
Professor of Naval Warfare Studies

____________________ ________
(Faculty Advisor) (Date)
Robert A. Coe, Lt Col, USAF
Joint Military Operations Department

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

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.

This new form of cyberspace brings both opportunities and challenges. Drawing sustenance from our rich pioneering heritage, the military must venture *off the trodden path.* We must move our concepts beyond the current "definitional round" of information warfare discussions. Changing division of labor equations between man and machine have led us to new interfaces, with which today's information warriors might gain entry into this new cyberspace. Unfortunately, these interfaces appear dedicated to maintaining the status quo--simulating traditional force employment, and supporting applications like data warehousing. Technological, organizational, and operational innovation might be enhanced by using these interfaces instead to *explore* the domain *from the inside*. This approach might facilitate further insight into the type of requirements necessary for navigating cyberspace's peaks and valleys, perhaps leading us to a new theory of victory.

Admittedly, we face a hard choice at the outset of our long road to information superiority: whether to stay with familiar tools and concepts or whether to make the effort to switch to potentially more useful applications. The payoff is the furtherance of our national security interests and a brighter tomorrow. Alas . . . we are a nation of explorers.

CHAPTER I

INTRODUCTION

Background.

This is a research paper for the purpose of generating knowledge about means for conducting operations in the information domain. If the information domain is a *place*—similar to land, air, sea, and space—as some senior military leaders suggest, then it follows that joint warfighters will need coordinates and a mapping system similar to those used in the more *natural* domains.[1] If one assumes that the information domain is a 'place like any other,' then not only does the military sector lack a context for presenting this place; they lack key navigational devices necessary for its *exploration*.

Observations from recent national security and military exercises like RAND's *The Day After* and USACOM's *Evident Surprise*, as well as those from senior leaders and operators summon one to find a context for this new realm. One can draw explicit and implicit imperatives from these observations such as the need for visualization of information dynamics and resources; geo-location and positioning of resources; simultaneous system operation and analysis; integration and synchronization with other domains; and collaboration within the domain. By thinking through these imperatives, both commanders and operators can gain vital insight into how to prosecute future information warfare (IW) campaigns.

---

[1] Hayden, Major General Michael V. "Information Operations, Information Warfare, Intelligence, briefing, April, 1996." As one of the principals charged with its current monitoring and analysis, Air Intelligence Agency Commander, Major General Hayden offers that the information domain is a place to conduct operations similar to land, sea, air and space.

The academic and commercial sectors quickly realized the monetary and social value of more closely examining this new domain, which is alternately referred to as cyberspace in this paper. Development engineers from these sectors have continued to move beyond the "flat-screen" computer to more advanced interfaces. More recently, they have investigated the entire human body and the senses as potential mechanisms to navigate, communicate, and move objects in this new domain. They hope that these new, more intuitive interfaces will not only provide entry into this *innerspace*, but will enable them to traverse its peaks and valleys.[2]

The exploration of this new domain will require interested parties bringing together varying and seemingly unrelated disciplines. Researchers from these disciplines realize that they can no longer independently observe the tasks of navigation and examination of information spaces. They are beginning to understand that a more dynamic kind of interaction--an *exploration*--may be necessary.[3] For example, researchers from the field of geography recognize that the topography of this new domain is becoming a more important field of research than the classical units based on study of the natural domain—land, sea, air, and outerspace.[4] A new inter-disciplinary approach promises to combine

[2] The concept of inner space as an analog to outerspace is introduced here and used throughout the paper. The author intends this term to be synonymous with "information domain" and "cyberspace."

[3] Dr. Creve Maples, Vice President/Operations, MuSE Technologies Incorporated, discussion with author, 10 December 1996, Albuquerque, New Mexico. Dr. Maples explains that *exploration* involves more than just mere navigation, and more than just mere examination. It is a combination of various areas of human-computer interaction, such as navigation, presentation, interaction, and examination. These areas should form a functional arena for interactive environments and provide a foundation for the type of tools to be used in this environment.

[4] Julie Ryan and Gary Federici, Offensive Information Warfare - A Concept Exploration, Center for Naval Analysis,Alexandria, VA: Jul 1994, research paper, 16. The author uses the term "outerspace" rather than the more popular term "space" in this paper to describe this warfighting domain. The author prefers to use the term in its more general usage as a reference to "time and distance."

aspects of geography, communications, and user interfaces.[5] By crosscutting discussion of these varying disciplines with principles from science and warfare, military development engineers can also gain new insights into the problem.

Military members can be expected to engage in conflict in the information domain like any other. In fact, warfare within this new frontier has emerged as one of the principal US national security concerns. The Joint Security Commission describes US vulnerability to warfare in the information domain as "the major security challenge of this decade and possibly the next century."[6] Larry Merritt, the Technical Director of the Air Force Information Warfare Center (AFIWC) worries that "we lack a common canvas from which to work from, in the face of an increasing rate of electronic intrusions and incidents in this domain."[7] Additionally, recent panels and task forces have been increasingly critical of current Department of Defense (DOD) practices and assumptions about the information domain, and are recommending that the Pentagon be given the legal ability to "repel and pursue those who try to hack into DOD computer systems."[8] The military is not the only laggard. Academics are already suggesting to each other that industrial-age experiences and tools may not be as effective in the information age.[9]

---

[5] Mason Takeyama, "Toward Cybergeography: A Proposal," undated, <http://www.sfc.keio. ac...ography /proposal_e.html> (30 November 1996).

[6] Major Richard W. Aldrich, "The International Legal Implications of Information Warfare," Airpower Journal, (Fall 1996): 100.

[7] Larry Merritt, Technical Director, Air Force Information Warfare Center, interview by author, 10 December 1996, Kelly AFB, San Antonio, Texas.

[8] Thomas E. Ricks, "Information-Warfare Defense Is Urged," Wall Street Journal, 6 January 1997, B2. Legal, security and cost concerns are the prevailing reasons given by those in the field for lack of progress in the exploration of the domain.

[9] AFCEA International Press 1996, CyberWar: Security, Strategy and Conflict in the Information Age - Introduction, eds. Col. Alan D. Campen, USAF (Ret.), Douglas H. Dearth and R. Thomas Gooden, <http://www.us.net/signal/AIP/intro.html> lkd. <http://www.us.net/signal/> (19 December 1996).

In the summer of 1994, information operators witnessed these challenges first-hand while helping the AFIWC Commander build a briefing on an information mission for senior Air Force officers in Washington, DC. Their task was to create a briefing, which conceptually portrayed events during a hacker attack on information resources at Gunter AFS, Alabama. It was during these preparations that they realized they lacked a *context* for warfare in this domain. Our explanation to the SECAF felt anticlimactic, relied on analogs to the air domain—detect, identify, intercept, destroy—and failed to show the dynamics of the attack and the unique nature of operations in the domain.

It was during this search to explain *how it went* to the SECAF that AFIWC operators reflected on important questions. How might operators more effectively present similar scenarios to senior decision-makers or joint force commanders in the future? More importantly, will today's devices wielded by young operators be sufficient in the face of a more concerted onslaught of multiple information attacks?[10] How might the same cadre of information operators and decision-makers have fared if they had tried to command and control the defense and response to an increased number of simultaneous attacks using traditional computer and communications tools? Will future information operators continue to rely on describing and reacting to critical national security events via a secure phone system and their own divergent views of a consensual space? Will future information operators rely more heavily on expanded *exploration* vice more traditional intelligence *examination* skills?

[10] Merritt, interview. Mr. Merritt reports that as of the date of interview the AFIWC responded to over 4,150 incidents at the time of the interview in 1996. Recently there were over 200 attempts at intrusion at 19 Air Force sites. He suggests that the number and the nature of attacks—concerted attack from nation states—will continue to rise exponentially.

Daunting problems of time and space have never held military explorers back before. A rich military tradition of exploration exists in the United States, dating back to George Washington, all the way through Admiral Peary, to the men and women of the present NASA space program (see figure 1-1.). These pioneers ventured off the trodden path, into the void spaces of the world for various reasons: adventure, a keen thirst for scientific knowledge, and the mysterious fascination of the unknown.[11] One might recall that the present-day Internet, the 'network of networks,' sprung from ARPANET, the backbone computer network of the Defense Advanced Research Projects Agency. [12] It is only fitting that the DOD should be at the forefront of the exploration of the information domain, a large part of which it was responsible for creating. Instead of merely transiting cyberspace, the military will need to operate within it to find new meaning for a new type of conflict—*netwar* in a synthetic information domain.[13]

Most military research on synthetic environments seems focused on providing either "dominant battlespace awareness" or "dominant battlespace knowledge (DBK)"—geared to a broad command and control capability spanning all of the warfighting domains. Yet, after only a few years since its introduction, the DBK approach seems too amorphous, broad and convoluted. Therefore this paper concentrates on a small subset of

---

[11] Lieutenant Ernest H. Shackleton, "The Heart of the Antarctic," National Geographic Magazine: An Illustrated Monthly, Vol XX (1909): 972. Lieutenant Shackleton, USN, led the South Pole Expedition of 1908-09, which reached a point only 110 miles from the South Pole.

[12] Michael Batty and Bob Barr, "The Electronic Frontier: Exploring and Mapping Cyberspace," Futures, 26(7) (1994): 700. ARPANET was originally part the US Department of Defense's bid to keep their computers running in the event of nuclear war.

[13] John J. Arquilla and David F. Ronfeldt, "Cyberwar Is Coming!" Comparative Strategy, 12, n. 2, (1993): 146. Arquilla and Ronfeldt, RAND analysts, describe *netwar* as ". . . infiltration of computer networks and databases," and offer they are "distinguished by their targeting of information and communications."

these challenges, attempting to work up from that 'corner' of the battlespace currently dedicated to netwar.

PHOTO COURTESY OF NATIONAL GEOGRAPHIC MAGAZINE

Figure 1-1 - Admiral Peary at the North Pole

This study examines current theoretical and practical frameworks and metaphors used to describe cyberspace by extending, generalizing, and at times negating traditional geographic principles. This paper hypothesizes that a more intuitive or 'multisensory' approach may be the best way to organize and present information for operators in this domain. It examines present and potential methodologies for not only domain presentation, but also domain navigation. Additionally, the paper delves into implicit information warfare requirements that have surfaced only in the last few years.

Assumptions. Though one cannot predict the future, one can make assumptions about the future and act upon these assumptions.[14] For the purposes of this paper, one might not only assume that the 'information domain' is a place, but that it is a *real* place or domain. Martin Plewe, a noted geographer at the University of Colorado, notes that "a geographic domain is a space in which traditional concepts associated with geographic thought--spatial distribution of economic, cultural, physical and other phenomena in relation to human beings--have meaning and application."[15] Curiously, many of today's authors refer to cyberspace as somehow not being physical or real. Anyone who has ever seen a group of preteenagers huddled around a video game console in a neighborhood arcade knows their actions are plenty physical.[16] Working in the future information domain will be no less real to the information operator than to the air operators in other domains.

Even if one does not accept that cyberspace is a real place, research and analysis of recent exercises involving US government senior officials would seem to confirm that we are treating it as it were real. Additionally, one would hope that development engineers are attempting to enhance "total reality," rather than building unreal information spaces or

---

[14] M. Ethan Katsh, Cybertime, Cyberspace and Cyberlaw (Article 1), <http://lii.cornell.edu/jol/katsh.htm> (19 November 1996). Katsh is a Professor of Legal Studies, University of Massachusetts at Amherst.
[15] Brandon Plewe, "A Geography of Cyberspace: Is the Virtual World as Spatial as the Real World?," Geography 666, Spring 1995, University of Colorado, <http://www.geog.buffalo.edu%7 Eplewe /cyberspace/> lkd. Martin Dodge,"Geography of Cyberspace: Some Other Useful References," 25 Nov 1996, <http://www.geog.ucl.ac.uk/casa/martin/ geography_of_cyberspace.html> (19 Nov 1996).
[16] Philip Elmer-DeWitt, "Welcome to Cyberspace: What Is It? Where Is It? When Can We Go?," Time Domestic, Special Issue, Spring 1995 Vol. 145, No 12, <http:pathfinder.com/@@zHGstAYA3U5ˣbeKK/ time/magazine/domestic/1995/special/tspecial.cover.htm> (28 Nov 95) lkd. Martin Dodge, Geography: Some Other References , 25 Nov 1996, <http://www.geog.ucl.ac.uk/casa/martin /geography _of_ cyberspace.html>. Elmer-DeWitt notes that when William Gibson, the author of the science fiction novel *Neuromancer*, wandered past video arcades on Vancouver's Granville Street in the early 1980's he noted something peculiar about the way players were hunched over their glowing screens, and that they 'believed in the space the games projected.'

simply augmenting physical reality "from the outside."[17] The interaction and integration of the natural world and the synthetic world promises to be a critical requirement for future military expeditions into innerspace.

The information domain embodies something larger than the Internet, and as a term should be indistinguishable from either cyberspace or innerspace. Many researchers have observed that the Internet is merely an attempt to give body to the information domain and represents a "network of networks" that provides the temporary skeleton for cyberspace.[18] The propositions forwarded in this paper might not only apply to near-term netwar, but to a full-scale cyberwar in the distant future.[19]

This study does not to describe the symbology, features, etc., of the broader area of information-based warfare.[20] Such a scenario might exist somewhere between the environment described by Winn Schwartau, author of the book *Information Warfare: Chaos On the Electronic Superhighway*, who describes information warfare as "an electronic conflict in which information is a strategic asset worthy of conquest or destruction" and that of *netwar* described by RAND's John Arquilla and David Ronfeldt.[21] This research envisions activities that are not limited to "information gathering" but also

[17] Scientific American, Inventing the Future, episode #701, produced for GTE by Chedd-Angler Prods, 40 min, 23 October 1996, videocassette. This episode, hosted by Alan Alda, features a walk-through of the various inventions of MIT Media Lab researchers. In this narration Mr. Alda states that researchers at MIT are attempting to 'augment physical reality.'
[18] Batty and Barr, 700.
[19] Arquilla and Ronfeldt, 146. Cyberwar is similar to what NDU describes as 'information-*based* warfare' in that it refers to "conducting, and preparing to conduct military operations according to information-related principles."
[20] Aldrich, 101. The working definition of 'information-based warfare' recognized by National Defense University is: an approach to armed conflict focusing on the management and use of *all* information in *all* its forms and at *all* levels to achieve a decisive military advantage especially in the joint and combined environment.
[21] Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway, (New York: Thunder's Mouth Press, 1994), 13.

include the "give and take" of offensive and defensive information warfare at the tip of the information operations spear (see figure 1-2).

The antithesis to these views is that cyberspace is not "a place" and hence there is no need for the military to explore it from the inside. Still others grant that the information domain is a place, but suggest that the military will never be able to fully represent its activities in real time. Some authors such as National Defense University's Martin Libicki, question the applicability of traditional disciplines such as geography to

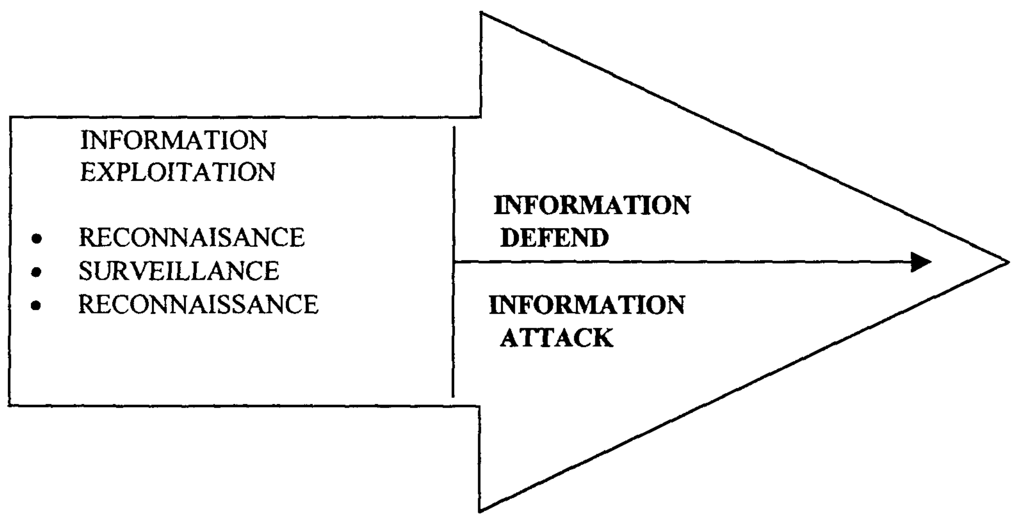


DIAGRAM COURTESY OF AIA/CSX

Figure 1-2 - The Tip of the Information Operations Spear

Cyberspace, while others suggest we'll never be able too fully model it for the conduct of operations.[22] Others propose that non-spatiality is one of the fundamentals of cyberspace,

[22] Martin Libicki:, "The Emerging Primacy of Information," The National Interest, Spring 1996, 261.

and a harbinger of the 'death of distance.'[23] Some claim that it may one day be a place, but given the new relationship between time and space, it may be impossible to conceptualize the domain with today's capabilities. They offer that in today's unshaped realm, it is possible for one person to be simultaneously interacting with six different computers, while inhabiting six different personas.[24]

Though a strong belief that doing more in less time is beginning to pervade society and the military, one cannot afford to overlook spatial considerations in cyberspace. This research and analysis assumes that spatial orientation will remain an important factor for conflict in this domain. In fact, many commercial enterprises in the United Kingdom, and the United States hope that "space is money;" that economic rewards will derive from developing and exploiting novel relationships and new capabilities for overcoming constraints of space and distance.[25] To those skeptics who would argue that time pressures obviate any conceptualization of cyberspace, one might offer that many informed observers still believe that time will remain *actionable*. In fact, James Gleick, the noted scientist, observes:

> The problem is, even a second is long—not 'an instant' anymore. It stretches out before us as a container, with events and voids to be filled with milli-, nano- or picothings. A second is long enough for impatience to begin welling up.[26]

There are very few applications at present that can take all the digital data an organization works with and represent them in a multisensory space. Yet, given the

---

[23] "The Death of Distance," Economist, 30 September 1995, 6.
[24] Alan Wexelblatt, Research Assistant, interview by author, 3 December 1996, Intelligent Agents Section, MIT Media Lab, Cambridge, Massachusetts. Mr. Wexelblat relates that Ms. Sherry Terkle and other MIT researchers have conducted extensive research regarding 'personas in cyberspace,' which appear to support this view.

advances in communications and information technologies it might be reasonable to assume that joint warfighters will soon be able to utilize custom-made operating environments from the commercial sector which wrap around differing hardware and software applications. By Christmas of 1997, every personal computer on the market will have a three-dimensional (3D) graphics card installed whether users like it or not.[27] The "multi-sensory threshold" appears to be next. Yet, some information technologists remain cautious about even strictly three-dimensional (3D) presentation, offering that human spatial talents operate best in a consistent environment, with consistent spatial placement.[28] They caution that 'flying around' in cyberspace not only offers an opportunity to access new data but also to get terribly confused and lost--what the military classically refers to as 'friction' in a campaign.

Today's information engineers and architects, using the 'mortar' supplied by 3D graphics, face an environment not unlike the software development environment in the 70's—the hardware is changing very rapidly, software standards are still trying to stabilize, and the construction of graphic representations is very time consuming.[29] For those attempting to develop synthetic environments, the situation is even more difficult. The demand for real-time operation—*beyond modeling and simulation*—and the need to support a more sophisticated level of user interaction make this one of the most difficult and challenging areas in the computing arena.[30]

---

[25] Katsh. WWW.
[26] James Gleick, "Just A Damn Minute," New York Times Magazine, 14 May 1995, 12.
[27] Andrews, discussion.
[28] Dr. Richard Bolt, Senior Research Scientist/Program Manager, interview by author, 3 December 1996, MIT Media Lab, Cambridge, Massachusetts.
[29] MuSE Tech, WWW.
[30] MuSE Tech, WWW.

CHAPTER II

GEOGRAPHY AND THE INFORMATION DOMAIN

Characterizing the Domain

It is especially important for national security officials, commanders and operators to consider how contemporary geographers and engineers are characterizing the topography of cyberspace. Courses on "Interpreting Cyberspace" and "Cyber-geography" are popping up in college curricula across the country.[31] For the military, these interpretations or characterizations can provide great insight into leverage areas for future warfare. The great military strategist, Carl Von Clausewitz offered that: "Topographies are important because they impose distinctive constraints and provide distinctive opportunities that have profound implications for policy and strategy."[32] Military opportunities to influence the ongoing construction and transformation of cyberspace—where there are no givens regarding history, geography, and environment—appear even greater than those with the land, sea, air, and space domains. Recent national security exercises like RAND's *The Day After . . . in Cyberspace II*, and USACOM's *Evident Surprise*, involving some of the nation's senior decisionmakers, have already revealed useful insights for characterizing the information domain. Concepts such as safe havens 'and other terms related to the tasks of 'locating,' pursuing or 'tracking' items in

[31] One such curriculum offered in the fall of 1995, by the University of Pennsylvania English Department, was entitled "Interpreting Cyberspace: Explorations in Virtual Geography" <http://dept.english.upenn.edu/ ~sgarfink/eng9/syllabus.html> (27 November 1996).

[32] Carl Von Clausewitz, On War, edited by Michael Howard and Peter Paret, (Princeton: Princeton University Press, 1984), 348.

cyberspace are geographic in nature.[33] Further they point to the potential utility of a coordinate system or a map to operate in this new realm.

Beyond Clausewitz, science fiction, and recent interface advances, the military also needs to consider how principles of science fact might be used to characterize the new domain. Already new rules and laws of cyberspace are being derived from the first pioneers from the constraints and opportunities of broader physical reality as well as the limitations of computing and electronic communications.[34] Like any other domain, new principles of cyberspace will ultimately be formed that would seem alien to its first generation of explorers.

A Place. Though a geographical setting does not determine the course of history, it is fundamental to all that happens within its boundaries.[35] This ongoing characterization of the information domain by the academic, commercial, and even domestic sectors will prove instrumental to how the military conducts future information operations. Rather than engaging in philosophical debate about whether cyberspace is a place it may be more productive to examine whether it is a place like any other. The fact that cyberspace is of synthetic or man-made rather than natural origin should not exclude it from being considered 'a place like any other.' The contemporary study of geography has evolved to consider borders, boundaries, objects and actors in both types of settings. Further, the world's leading geographers broadly agree that we need to start making maps of this

---

[33] Rand. "The Day After Summary," 7 November 1996), photocopied.

[34] Michael Benedikt, "Cyberspace: Some Proposals," chap. in Cyberspace: First Steps (Cambridge: MIT Press, 1991), ed. Michael Benedikt, (Cambridge: MIT Press, 1991), 132. In his article Benedikt, using what he describes as "low-altitude mathematics," outlines seven principles from natural domains which can be used to explain behavior in cyberspace: *exclusion, maximal exclusion, indifference, scale, transit, personal visibility, and commonality.*

[35] Colin S. Gray, "The Continued Primacy of Geography," The National Interest, (Spring 1996): 248.

newly-discovered, and newly-created multidimensional space, and that to do so, one must think differently.[36]

How did the term cyberspace originate? Science fiction writer William Gibson first introduced the term to a mass audience in his 1984 novel *Neuromancer*.[37] Gibson sought to describe his vision of a global computer network, linking all people, machines, and sources of information in the world through which one could navigate as through a synthetic space. Gibson compared this seemingly distributed "space" of information, as well as its owners, within the computers and networks, to people and places in the external or natural world.[38] One could argue that the world is rapidly approaching Gibson's vision. Research and analysis reveals that if current construction trends continue, banking, law enforcement, telephone, and other networks will soon overlay and interconnect with today's major webs of connectivity such as the World Wide Web (WWW).

A growing number of engineers and geographers are attempting to breathe life into the vision of Gibson and other science fiction writers. Hundreds of thousands of participants worldwide are using familiar spatial concepts to explain their experience in

---

[36] J. Morgan Reid, "Toward a Mapping of Cyberspace: Power, Creative Control, and Representation in the Postfordist Nexus," photocopy from Advanced Center for Spatial Analysis, University College London, UK, 1996.

[37] William Gibson, Neuromancer. New York: Ace Books, 1984. Gibson actually used the term previously in a lesser known science fiction story entitled "Burning Chrome." In this work, Gibson originally described operators using devices called 'cyberdecks' to override their normal sensory organs, presenting them with full-sensory interface to the world computer network; when doing so said users were in 'cyberspace.'[37] A similar *concept* was described prior to Gibson by Vernor Vinge in his novel *True Names*.

[38] Plewe, WWW.

cyberspace such as chat 'rooms,' 'public forums,' and place-based on-line communities.[39] They are attempting to 'gain entry' to this space with new interface devices.

Last year at a world conference on synthetic environments in Stuttgart, Germany, representatives from Division Ltd and Hewlett-Packard demonstrated the potential for the exploration of cyberspace of these new interfaces for a crowd of several hundred attendees from some of the world's leading research institutes, entertainment enterprises and corporations. The crowd was amazed as a huge display screen at the front of Stuttgart's Kultur-and Kongresszentrum Liederhalle captured the synthetic embodiments of three gentlemen from different points on the globe working together on an automotive engine. They were all wearing immersive headgear devices which projected them into a common three-dimensional plane, where they could not only 'see' each other but could pass tools back and forth (see figure 2-1). This powerful experience and several others where one could don similar headgear to work on simple tasks in synthetic spaces, lead one to conclude that there just might be a place *behind* the computer window, and a decidedly unique experience as well. Additionally, one could observe from the cross-section of international interest that the potential implications of synthetic environments were much bigger than Walt Disney and video games.

It is essential for information operators to understand also the larger changes in scientific principles which apply to all domains of conflict. One novel area of scientific inquiry which promises to affect how one characterizes this new domain is the study of chaos and criticality theory. Chaos theory, emerging only in the last three decades,

[39] Leslie Miller, "Bringing A 3-D Experience to the Internet," USA Today, 9 January 1997, 8D.

postulates that structure and stability lie buried within apparently random, nonlinear processes.

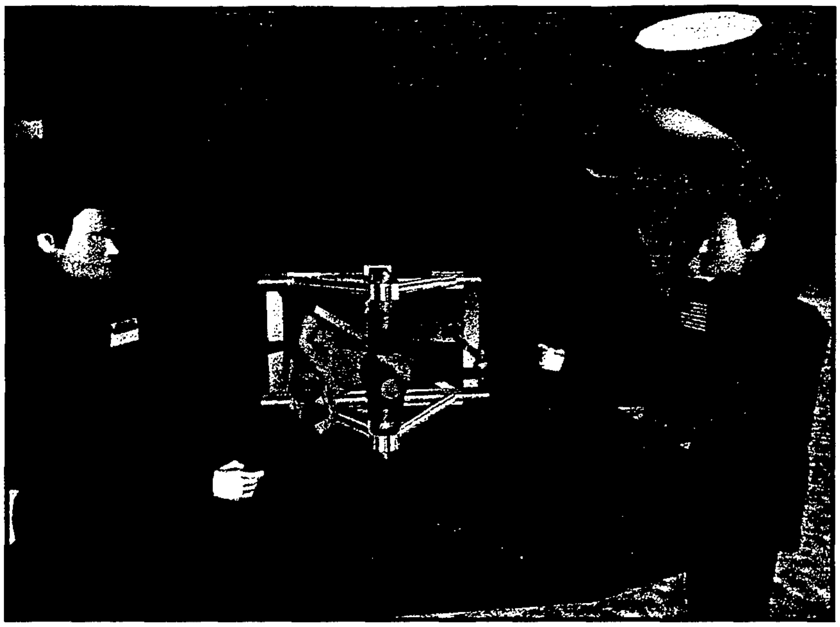


PHOTO COURTESY OF DIVSION LTD, BRISTOL, UK

Figure 2-1 - Collaborative Work in a Synthetic Information Space

Information operators at the AFIWC and the Defense Information Systems Agency (DISA) have intuitively realized this complexity since the initial hacker attack on US information resources. Complexity, randomness, and nonlinearity already appear to be central features of information warfare, where an increasing rate of attacks already suggests the need to bring order to a synthetic information domain. Chaos theory tells us that in the natural world, small events may have a disproportionate impact on the activities or behavior of an entire system. Perhaps in the future, hacker attacks, which appear random might conform to a larger pattern. Theories used to explain behavior in the natural domains might prove useful in the "inner" synthetic world as well.

In this regard, the military is confronted with a basic but important question: whether this new domain is characterized as chaotic or linear. The answer to this question will have great implications for the type of interface devices which operators use to gain entry into cyberspace. Author Stephen Mann, in his article, *Chaos Theory and Strategic Thought* observes that one might either view the process of battle as fundamentally chaotic, but moderated to an orderly system with varying degrees of success or as fundamentally linear and *non*chaotic, asserting that it is our individual perceptions of battle that are disorderly.[40] If it turns out one's perceptions of the battle are disorderly, as experience from today's information warriors suggest, then the military will not only be faced with considering the new features of this topography, but how to bring coherency to the perceptions of operators in this new realm through the use of more advanced devices.

In the past few years, social commentators have grappled with apt metaphors for cyberspace—mostly from the land domain--which geographers accepted warily as they weaved their way through its paradoxes. At first, commentators used familiar metaphors such as 'the information highway' to posit this new place, perhaps soothing an unfamiliar society's fears of inconsistency and instability. Today's pioneers, at every level of the military, are no strangers to these fears. Day-by-day, they continue their struggle of grappling with spatial and temporal terms and metaphors from across the spectrum of military operations to help characterize this new frontier for senior leaders and a growing legion of fellow operators.

Like Any Other. The comparison of the information domain as an analog to other warfighting domains provides a useful frame of reference. Though its horizons are unclear

[40] Mann, 60.

at present, one can probably assume that cyberspace will probably have objects, actors and content like any other domain. Travelers through cyberspace will take cues from other domains just as sea travelers take cues from natural objects on the horizon of land and outerspace.

What other domain is cyberspace most like? For years, metaphors such as the information highway have captured the public's imagination, implicitly indicating a preference for a land analog. Yet, research and analysis indicates that if cyberspace is to feature the same freedom of movement inherent to other domains, and so essential to the conduct of military maneuvers, it might be more beneficial to characterize it as a voluminous space similar to outerspace. Outerspace would seem to offer one the same panoramic experience of the past, present and future which they have come to expect from cyberspace. Observers have already come to regard cyberspace as less 'fixed' than the air, land, and sea domains, and hence more of a continuum.[41]

As the military, mirroring the transformation of attitudes and expectations in society at large, becomes more comfortable with the idea of this domain as a real place, operators will develop first principles to stake out boundaries, borders and zones of operation. Figure 2-2 provides a concept of how simple zoning principles used in military operations today, might be applied to the information domain.[42]

---

[41] Wexelblat, interview.

[42] US Joint Staff, J-7 Joint Doctrine Division, Joint Publication 1-02, Operational Plans and Interoperability, Washington: 33. In military parlance, an *area of influence* is a geographic area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. An *area of interest* is that area of concern to the commander to include the area of influence, areas adjacent thereto and extending into enemy territory to the objectives of the current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission.

Today's geographers are currently performing extensive research to determine whether the principles of geography can be used to explore to a synthetic cyberspace similar to natural spaces, or whether they need new ones.[43] The concept of core, periphery, borders, and boundaries are central to geometrical and geographical thinking and can readily be applied to information warfare. Perhaps the core for synthetic information operations space might be what RAND *Day After* participants termed the Minimal Essential Information Infrastructure (MEI)—or critical US information resources. Perhaps this MEI or core can be represented by a spherical, opaque shape around which all other objects rotate as shown in figure 2-2. This would resemble how we position and map objects floating around the earth in the present outerspace domain.

Perhaps due to intense time pressures, today's travelers, focused primarily on the transiting the links between the represented nodes of cyberspace, may be missing an opportunity to gain insight into the inner workings of cyberspace that come from exploring its new topographies. Traditional boundaries, whether they are physical, territorial or conceptual, appear more porous in an age where the majority of one's information appears in digital form. Research and analysis point out that the observation of cyberspace as "a borderless and boundless space" may not be entirely warranted. Though by its nature cyberspace does allow its inhabitants to transit existing natural spatial and temporal borders and barriers, the information domain itself seems to have *boundaries*. Cyberspace may appear to be infinite, but upon further exploration geographers are

[43] Plewe, WWW.

increasingly able to recognize the potential for consistent *boundaries* and patterns common to any other domain.[44]

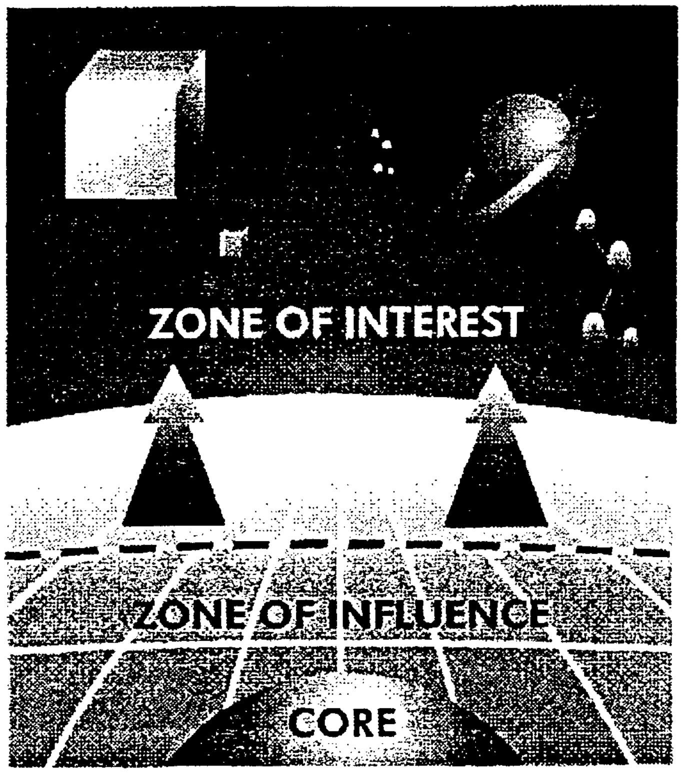


DIAGRAM COURTESY OF NWC GRAPHICS DEPT

Figure 2-2 - First Principles - Zone of Influence, Zone of Interest

Unlike Any Other. Despite attempts by the commercial, academic, and military sectors to compare cyberspace to the natural domains, cyberspace may be fundamentally

[44] Luc Girardin, Cyberspace Geography Visualization, PDF format report, Graduate Institute of International Studies, Geneva, 15 October 1995, <URL: http://heiwww.unige.ch/girardin/cgv/> lkd. Martin Dodge "Geography of Cyberspace: Some Other Useful References," 25 November 1996 <http://www. cf.ac.uk/uwcc/cplan/martin/g...cyberspace/geography_of_cyberspace.html> (15 Dec 1996).

unlike these other places. Unlike other domains—land, sea, air, and space—its canvas is not as manifest; i.e. it has not been fully brought to life as a medium of conflict. In fact, some observers have ascribed the 'death of distance' as one of the principal features of the new domain, while others steadfastly argue that spatial considerations remain relevant.[45]

Unlike the present focus in the air domain on speeding up information-related processes, the focus in the information domain will be presenting the results of a different *sense* of past and present, of the role and value of the past, and even a different series of concerns about the future. As discussed above, in the information domain, space appears to be an abundant resource much as in extraterrestrial space, yet time appears to be in somewhat scarcer supply.[46] It is with regard to time that cyberspace may be most unlike other domains. Past, present, and future are increasingly merged together in cyberspace. Evidence of a change in human perception of time can be gained merely by surfing the present-day Internet. Old and new documents at a website sit side by side, blurring any distinction between present and past. One can also examine the inner confines of the computer to find more evidence. A computer program spends energy feeding the past back into the present because this is an economical way for the system to deal with the future.[47] One of the first principles of computing is that a constant pulse of the past along the feedback loops informs and controls the future.[48] If the information domain is less limited by space and time than the other domains, its man-made construct may allow military operators potentially to control and *use* time to an even greater advantage than

[45] "The Death of Distance," 6.
[46] Katsh, WWW.
[47] Katsh, WWW.
[48] Ibid

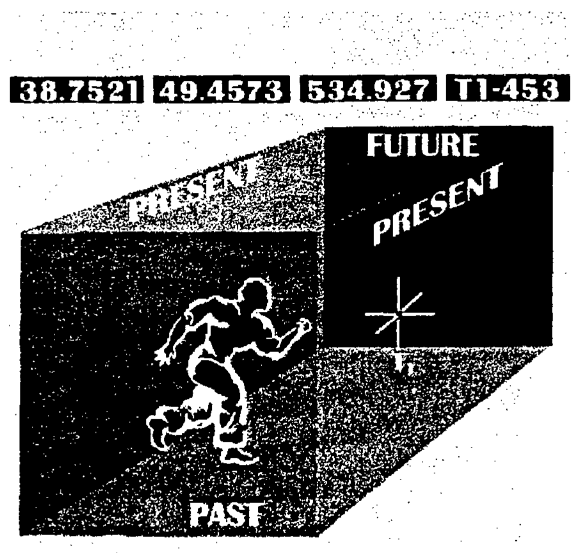
that allowed for in other domains. In the information domain, as opposed to the air, land, sea, and maybe space domains, time may be more about frames, than limits.

Ultimately the question of how to characterize and portray these unique relationships will come to the forefront. This will require new intuitive concepts for integrating space and time for decisionmakers. In an attempt to come to grips with the merger of geography and wisdom with a proposal for a learning cube to facilitate better decisionmaking by operators. This mechanism might overcome the inherent constraints of 'network' presentations which occlude considerations of intuition as well as past, present, and future (see figure 2-3). Perhaps a future operator might utilize a synthetic learning voxel--set aside from the fray of a cyber battle--for special scenarios requiring extreme focus or rapt attention.[49] In figure 2-3, an operator weighs the importance of the past, to determine its use in the present in determining the future--an operational dilemma that may confront operators. Inside the voxel itself, domain controllers have displayed time frames enabling the operator to more easily blend previously confusing temporal considerations.

There also may be distinct differences between the information domain and other domains with regard to modeling and simulation. Present modeling and simulation efforts are aimed from the top-down commander's perspective of the entire battlespace or one of four natural warfighting domains. (The corner of the battlespace dedicated to netwar has received short shrift in modeling and simulation efforts.) Yet in a synthetic information domain an *operator's* perspective may reign supreme in one situation and a commander's

[49] Benedikt, 155. Benedikt relates that in 2-D space, there are a finite number of finite-sized pixels on any video monitor screen, and it is not unreasonable to define the real size/area of an object as the absolute number of pixels that comprise it. Three-dimensional pixels are termed voxels (volume-pixel). Manipulating the density of voxels , will change the motion/behavior of the particle in a manner fully equivalent to a 2-D pixel case.

in another. Somehow these perspectives must be balanced by designers of new mapping and navigational devices.



DRAWING BY NWC GRAPHICS DEPT

Figure 2-3 - A Learning Voxel

Portraying the Domain.

Providing a frame of reference or characterizing cyberspace is necessary and useful, but the actual *portrayal* of cyberspace offers information architects an even greater challenge. One critical source of intuitive information for operators in cyberspace is, of course, the portrayal of the environment itself. This is where they will pick up those metaphorical, inferential, visceral, subliminal, and anomalous cues so critical not just to decisionmaking, but effective exploration—the task at hand.[50] If a domain is effectively portrayed, it can elicit new insights for the operator, especially if the domain is thought to

[50] Karen S. Peterson, "A Conscious Effort to Cultivate Intuition," USA Today, 26 November 1996, 9D.

be complex in nature. After examining what the information domain has in common with other domains and sketching a rough character, it is time to think about how one might present or portray the domain. *How* this topography is portrayed will be extremely important for how military operators conduct warfare in the domain.

Once the limitations of the natural world have been removed, then what? (A comforting note for prospective explorers is that few can definitively tell them *their* portrayal is wrong with any confidence.) With no limitations cyberspace could be a difficult place to comprehend, but perhaps not if one represents it in a logical, consistent way, which makes it useful for intuitive human functioning, which has served mankind ably throughout the ages. Whether cyberspace is presented as an expansive space or a network of links and nodes for will have great import on how a nation conducts warfare in the domain.

As the concept of information spaces has developed, so have attempts by academic, commercial and military researchers to visually portray and lend order to these spaces. Early attempts to map and explore even limited information spaces in the commercial sector were occupied with stability and linearity, perhaps due to customer fears. It was almost as if mainstream America recoiled from the disorienting ideas of the expansive cyberspace portrayed in science fiction novels like *Neuromancer* and *Snow Crash* and movies like *The Lawnmower Man* and *Tron*. Displays depicting cyberspace as a series of networks and links and nodes tied to a land topography began to dominate the commercial sector and the military followed suit. Usually these links and nodes are represented by computer positions in the natural world along with the layout of connecting cables, or by connected documents and screens where one can "drill down" through successive scenes for more detail. A new generation of geographers tell us that the network topology is excellent in overcoming distance but has relatively little concern with the past.[51]

Additionally, present military efforts related to the new field of information operations--shown in figure 1-2--mainly address the fusion or warehousing of intelligence, surveillance and reconnaissance (ISR) byproducts and not the dynamic environment expected in offensive and defensive netwar. Vice President Al Gore, who launched the present Global Information Infrastructure (GII) effort, has urged computer programmers to move beyond 'data warehousing efforts.'[52] In the face a mounting array of attacks on the Defense Information Infrastructure (DII), a traditional approach toward presentation what feels like a rich place, calling for exploration, is puzzling to say the least.[53] Information operators like Larry Merritt, the AFIWC's Technical Director, have learned from early skirmishes that in addition to functional systems that alert one to a virus in the network, they will need "intuitive functional displays for the next generation of decisionmakers, many of whom—in the short term--will be unschooled in the latest tactics and techniques of cyberspace.[54]"

It is clear that the old characterizations of cyberspace as a sort of highway are no longer useful. Many institutions are increasingly looking for better metaphors to describe

---

[51] Katsh, WWW.

[52] Gershon, Nahum and Judith Brown. Computer Graphics and Visualization in the Global Information Infrastructure, CG&A Special Report, Vol 16, No.2, March 1996, <http://www. computer.org/pubs/cg&a/report/g20060. htm> lkd. Martin Dodge, "Geography of Cyberspace: List of Documents," 25 November 1996, <http://www.cf.ac.uk/uwcc/cplan/ martin/g…cyberspace /geography_of_ cyberspace.html> (28 Nov 1996). Vice President Al Gore wrote the Opening Statement for this report.

[53] Merritt, interview. Mr. Merritt reports that as of the date of interview, the AFIWC has responded to over 4, 150 incidents that year. Recently were over 200 attempts at intrusion at 19 Air Force sites.

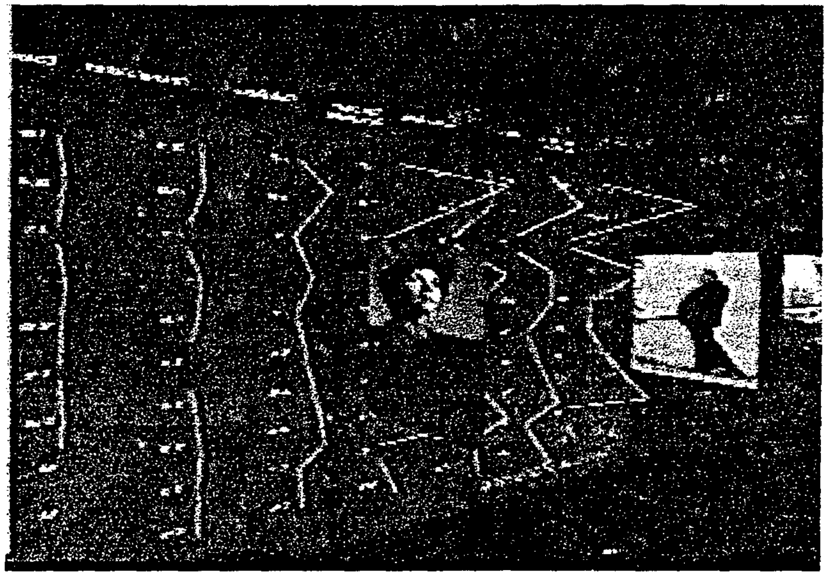
[54] Ibid

this *innerspace*. To make it accessible and to help us *think* better, researchers are already hard at work developing new spatial and temporal metaphors and models for operating in this domain which are less linear than concepts like the information highway.[55] They are also busy constructing spaces in which users can peruse information by navigating in and out, by using multiple human senses and intuitive capabilities.

Disregarding more traditional representations, researchers at MIT's Media Lab in the early 1980's seemed to start out with the proposition that information spaces were voluminous, yet required the imposition of a grid of some sort to lend stability and consistency. In the early 1990's, an MIT team under the guidance of Dr. Muriel Cooper, worked on an application called the Spatial Data Management System, a way bring order to information space. These portrayal utilized dynamic, transparent, intersecting planes to present complex information to executives and workers in commercial enterprises (see figure 2-3). Dr. Richard Bolt, a senior research scientist who worked on this project, related that important lessons learned about the mapping and navigating of new information spaces came out of this study. The team observed the necessity of reference points for consistency in such a voluminous space, fearing the operator would have no sense of 'up and down' and would be disabled from the resulting disorientation. Still, the Team's approach suggests that they assumed cyberspace extended into a volume of space beyond the desktop, as Gibson and others have envisioned.

Others such as French researcher Luc Girardin from the Graduate Institute of International Studies in Geneva, Switzerland, have ripped the traditional links and nodes

[55] Andrew McGrath, BT development engineer, interview by author, February 1996, Martlesham R&D Facility, Ipswich, UK.



COURTESY OF MIT MEDIA LAB

Figure 2-4 - MIT's Spatial Data Management System

used to represent networks from their land anchor; envisioning cyberspace as kind of a floating molecule one might recall from 7th grade science class. He has depicted perhaps the most developed corner of cyberspace, the World-Wide Web, as a graph, where each resource is a vertex and the links are the edges (see figure 2-5).[56] Girardin uses the distances between pairs of resources as a starting metric. With the ability provided to measure the distances among resources, he states it becomes possible to represent each resource as a point in a high dimensional space where their relative distances are preserved.[57] Yet, even Girardin's 'floating links and nodes' representation does not overcome critical limitations of networks.

If geographers are correct in their observations that space will be abundant in this new domain and time somewhat scarcer, it would appear a more voluminous space which

[56] Girardin, PDF format report.

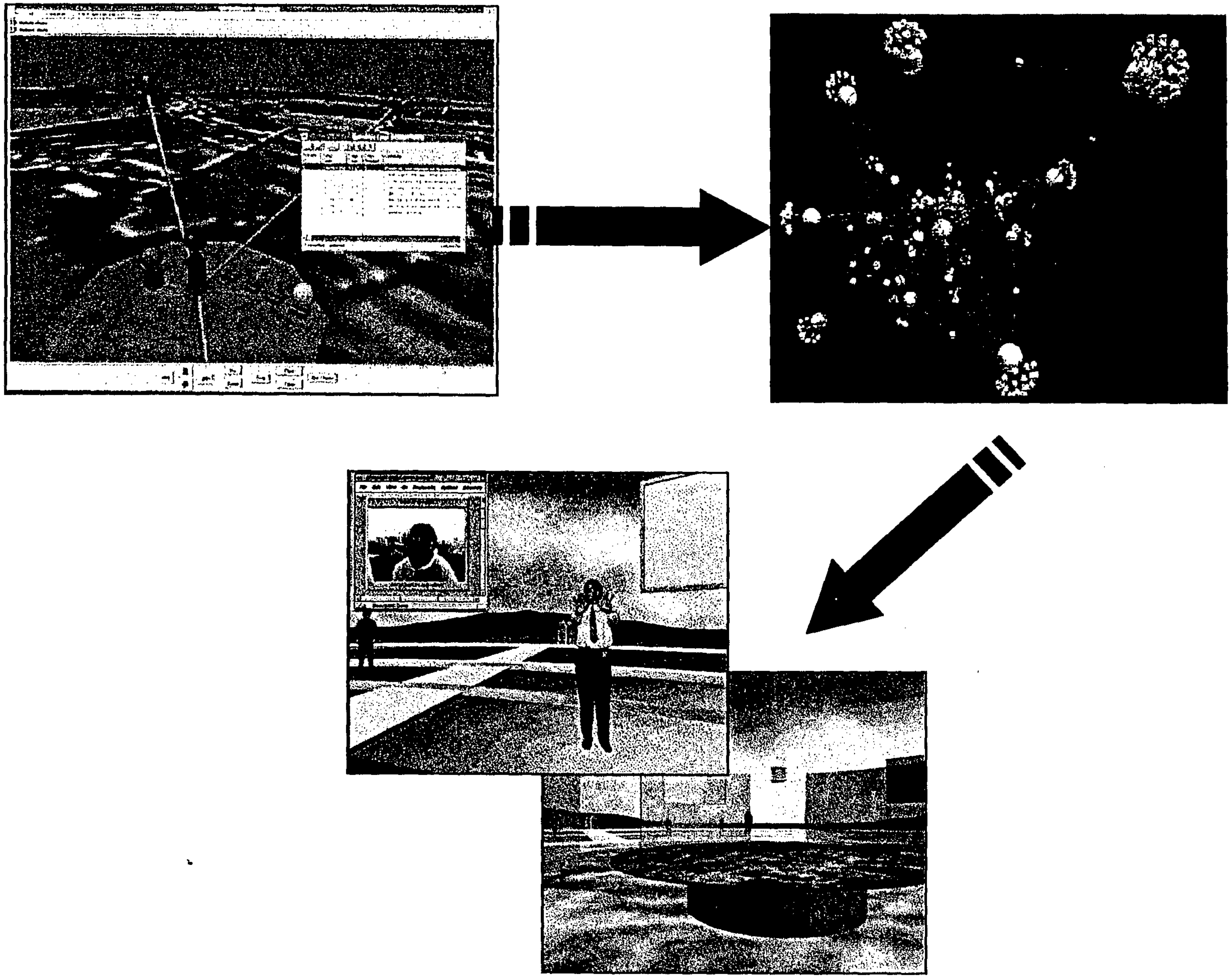
'pulls away' from the standard network method of representation might be a starting point. An approach that fits this bill is offered by development engineers from British Telecommunications. Rather than using standard land analogs to characterize cyberspace BT engineers are using innovative metaphors such as an *Infosea*, which better the reflect the dynamics of the everyday use of information. In this context they are looking at the construction of 'information islands' in a voluminous space where considerations of public and private space are merged (see figure 2-5). BT's development engineers theorize that the information domain will be a living, growing domain where unlike the natural world, informational resources will derive value from their ability to change over time and their ability to solve problems.[58] The benefits of an expansive visualizations of cyberspace that extend beyond the desktop such as *Infosea* are that they allow for better assessment, prioritization of threat engagement, area, value, and motion, than standard land-anchored network representation.

Military Application

As military officials have become more comfortable with the concept of cyberspace they have moved on to earmark tasks for future operators. One of the questions participants from RAND's *Day After* Exercise asked the US research and development (R&D) community for help with was whether with proper visualization would allow operators to detect abnormal patterns of IW activity before they became destructive.[59] Both lessons learned from this exercise and recent observations by the

---

[57] Girardin, PDF format report.
[58] Katsh, WWW.
[59] Arquilla and Ronfeldt.



PHOTOS COURTESY OF SENSE8, LUC GIRARDIN, AND BT

Figure 2-5 - Evolution of Information Domain Portrayal

AFIWC about prioritizing resources for information defense, point to the need for better tools for:

- Visualizing information flows
- Locating and positioning resources

Visualization of Information Resources. Visualization is a method of computing, that transforms the symbolic into the geometric, enabling researchers to observe their simulations and computations. Visualization offers a method for "seeing the unseen," in this case cyberspace.[60] New visual display means and interface devices pictured in figure 2-6 do not simply allow operators *entry* into cyberspace. They now allow operators to visualize information in three-dimensional space, to move through it and interact with it—experiences fundamentally different than those provided by the desktop computer. New display means have already been responsible for enriching the process of scientific discovery by fostering profound and unexpected insights. Their mere potential is why the 3-D commercial market is on the verge of an explosion in growth, and why leading companies like British Telecommunications are investing in both large and small-scale multi-dimensional presentation means for enhanced decisionmaking.[61]

Military contractors working close to the front lines of the information war, admit not only that the presentation of this new domain of conflict is critical, but that present display means are self-limiting and artificial. Mr. Roger Robinson, C^2 Protect Program Manager for Trident Systems, currently working on 21st century visual display tools for the AFIWC, admits that "We are not very effective today at making people aware of what's going on [in the information domain]." He relates that the simple Global Watch

Display System he is developing, " . . . is really about building links to other resources and nodes to first learn what it is that we are really protecting in the first place.[62]" As one part of the larger Global Watch effort, operators at the Air Force's Information Warfare Center (AFIWC) are working on the Generic Mapping Tool, a device that can provide a display of the status of USAF information assets across the globe, and refreshes itself every 30 seconds.[63] It is a two-dimensional (2D) computer desktop visualization anchored off a land-based geographic depiction of USAF informational networks.[64] Still, it enables an operator to "drill-down" from an overall network status all the way to nodes or hosts. One can't help but think that newer interface devices such as those featured in figure 2-6 might help AFIWC operators capture the true dynamics of cyberspace in a more effective manner than 'flat-screen' displays where important peripheral considerations can be displayed alongside core considerations. If actors and objects are visualized in the most effective manner, the operator's mind can be freed up to perform more critical tasks such as pattern recognition and anomaly detection for information defense.

If cyberspace is expansive in nature, then it may be more important for an operator to visualize and manipulate information *content*—actors, objects, resources--rather than simply redirecting information *flows* through networks. Reflecting on the development of high definition TV, Nicholas Negraponte, founder of MIT's Media Lab, asserted that research was misdirected at higher resolution pictures rather than improvements in the

---

[60] MuSE Tech, WWW.
[61] Ibid.
[62] Roger Robinson, Trident Data Systems, Development Engineer, Interview by Author, 11 December 1996,
Kelly AFB.
[63] Thatcher, interview.
[64] Ibid.

'artistry of content.'[65] What objects and actors will constitute the content of a future information domain? What resources or obstacles will be necessary for information architects to visualize?

While traversing the zone of interest, operators can be expected to move through an environment rich in content, among friendly, neutral and enemy actors, objects and obstacles. Clausewitz said that geography could affect military operations in three ways: as an obstacle to the approach, as an impediment to visibility and as cover from fire.[66] In the voluminous cyberspace of the future it might be possible for information operators to use objects such as those portrayed floating around cyberspace in figure 2-2, as *cover* from information attack. Award-winning science-fiction author Orson Scott Card's last novel *Ender's Game* featured a zero-sum gravity arena for warfighting training where cadets took advantage of various-shaped objects hovering a in zero-gravity game room to defeat opposing teams.[67] Warriors fighting in the future synthetic information domain might be expected to do the same with a wide-range of visualized objects.

The visualization and geo-location of objects in cyberspace will be important to any intuitive real-time display necessary to portray the rich environment described above. Objects within the friendly zone of influence might be programmed, sculpted or tagged with radiating properties that enable the operator to track more easily them for subsequent repositioning. When future standards evolve, it may well be that computer viruses and other information threats such as Trojan horses, logic bombs are presented as dynamic

---

[65] Frank B. Strickland Jr., "It's Not About Mousetraps-Measuring the Value of Knowledge for Operators," Joint Force Quarterly, Autumn 1996, 90-99.
[66] Clausewitz, 348.

icons resembling the shape, movement and relative pace one might expect from their counterparts in the natural world. There would appear to be a finite number of ways you could be attacked in cyberspace.[68] The key will be to figure out the various classes of attacks and weapons choices and represent these in some way. Architects will have to categorize the rates of speed of various information weapons and then give them relative representations to approximate these rates of speed. For example, in the distance, coming from the zone of interest, an operator may alert a commander that he has picked up the rough outline of a Trojan horse ambling toward the enemy core. Perhaps he lets an enemy worm slither by, knowing he can catch up and dispose of it later, choosing instead to block a much faster logic torpedo whirring at him.[69] Maybe a large conventional attack from a nation-state is distinguished from a normal hacker incident by an ominous audio clip from the JAWS soundtrack, or its hazy portrayal on the horizon of an operator's zone of interest. Operators might also wish to sow information mine fields around the core or outlying information resources they wish to protect. They might wish to alert each other to 'no strike' or 'no access' areas with visual and supplementary audio cues.

One would need to build-in to this domain methods of not only visual, but also geo-locational considerations. The concepts of 'core' and 'periphery,' discussed briefly

---

[67] Orson Scott Card, Ender's Game, New York: Tom Doherty Associates, 1991. Mr. Card won the prestigious Hugo Award, presented annually by the World Science Fiction Society for the previous year's top science-fiction novel.

[68] Dr. Arlan Andrews, Vice President/Marketing, MuSE Technologies Incorporated, interview by author, 6 December 1996, Albuquerque, New Mexico.

[69] David Alexander's article "Information Warfare and the Digitized Battlefield," in Military Technology Magazine, 9/95, has an excellent section on p. 63 entitled 'A Computer Virus Primer,' which describes three potential attack objects. A Trojan horse is a program hidden within a host program and triggered upon execution. The host program, may be a legitimate application which hides the Trojan. When placed on a system within the viral host, Trojan horses can replicate and spread across networks. A Worm is a program that bores through system memory, obliterating or altering data. Delivered as part of a virus,

earlier, are central to geographic geometries, and will be for positioning and redirecting US Minimal Essential Infrastructure (MEI) resources.[70] In the predominant coordinate system for outerspace used by engineers and scientists, the origin for locating bodies in space or the 'core' for reference is the center of the Earth.[71] Perhaps for 'core' for synthetic information operations space might be the MEI for the United States, represented by a spherical shape, which all other representations orbit around. For instance, Iran or Cuba might be represented as large, red-hot balls, at arm's length from the US core, reflecting the relative mental energy the nations spends on smaller threats—in the natural sense. On the other hand, one might imagine a neutral actor such as IBM represented by a big blue cube floating around cyberspace, with perhaps a red-hot ball inside it representing an Iranian expatriate known to be working in their advanced systems department. Perhaps everytime an operator sees a black cube one might expect an attack from Tokyo's 'Yokuza gang.'

Maintaining effective means of portraying any warfighting environments can have a significant payoff regarding national security questions. In apt testimony to the power of new presentational means, during an impasse in the Dayton peace accords, Bosnian President Izetbegovic was convinced to change his position when he was given a joystick to guide himself in a video flight over a small mountain path portrayed on a computer screen.[72] Effective as it was in this instance, the sheer amount of information humans are

---

worms can replicate with great speed. A logic bomb is a program that embeds itself in an executable file to lie dormant until a specific event, often a date, triggers it, upon which it becomes active.

[70] Robinson, paper.

[71] Major Michael J. Muolo, AU-18: Space Handbook An Analyst's Guide - Volume Two, Maxwell AFB, Alabama: December 1993.

[72] National Security Agency, "Pointers to the Latest News on Telecommunications and Computer Technology, " <http://192.13.244.99/ttn/5-1/pointers.html#HDR27> (9 April 1996).

increasingly facing is outpacing the flat screen as an adequate mechanism for processing information. If present trends continue, in 2015 there will be more than 5, 000 times more information in the world than there was in 1994.[73] To get ready this for this deluge, researchers in the academic, commercial, and military sectors are busy looking for new and more efficient ways to organize and present information. They are experimenting with new man-machine interfaces that amplify man's *capabilities*, not a separation of man and machine.[74] Further, a trend is evolving where engineers are adapting synthetic environments to operators rather than vice versa.

The increasingly familiar and somewhat cumbersome head-mounted display is shown on the top left of figure 2-6. Typically this device has a visor which extends to the operator's peripheral field of view. On the visor typically is presented a synthetic room or space of his choosing three-dimensionally displayed in front of him. Typically the operator wields a joystick device which lets him wander around the synthetic space which has replaced the natural space in front of him. Such a device lets operators dynamically alter their environment from within and move from one segment or portal of cyberspace the next, in effect putting the painter inside the painting. Another more stationary device which displays a similar scene is a binocular omni-oriented monitor (BOOM). BOOMs are devices that look like periscopes that are extended via arms from desktops or hang suspended from ceilings, freeing the operator from bulky headgear.

The middle photo in figure 2-6 represents an even less encumbered synthetic interface than a BOOM. This photo shows two operators interacting with IBM's *Rubber*

---

[73] John L. Peterson, "Information Warfare: the Future," chap. in Cyberwar: Security, Strategy, and and R. Thomas Gooden, (Conflict in the Information Age, eds. Col. Alan D. Campen, USAF (Ret.), Douglas H. Dearth Springfield: AFCEA International Press, 1996), 226.

Rocks application. Rubber Rocks is a synthetic space containing flexible objects. Operators can create, grab, hit, and shoot these objects using hand gestures, speech recognition, and sound generation.[75] Each operator is wearing a baseball cap with a position sensor for head-motion tracking, and a glove for gesture tracking. The two people in this picture are looking at a space from opposite sides. MIT Media Lab researchers have also worked for the last few years on a similar, but more unencumbered application called SURVIVE. Essentially like the magic mirror in *Alice and Wonderland*, the operator stands in front of a large display screen which rushes synthetic scenes past him in a gesture-driven adaptation of ID Software's now famous game DOOM. Similar to the *Rubber Rocks* application, his gestures are tracked only by passive sensors, in this case a video camera and a microphone. Yet, free of any attachments, he is merely required to gesture with a gun, which is tracked by the camera, and provides limited vector. This application tracks the user in three dimensions, without the user donning equipment.[76]

The third presentational device on the far right is Wright Laboratories vision of a surround-screen, surround-sound, projection-based synthetic environment. It represents a cylindrical adaptation of a system more commonly known as CAVE, which was introduced in 1992 by the Electronic Visualization Laboratory at the University of Illinois at Chicago. The CAVE is a synthetic theater consisting of an entire room constructed of large screens on which graphics are depicted in 3-D stereo onto two or three walls or on the floor. An operator wearing a location sensor similar to *Rubber Rocks*, moves within

[74] Arquilla and Ronfeldt, 147.

[75] IBM T.J. Watson Research Center, Yorktown Heights, NJ, Interactive Simulation in a Multi-Person Virtual World. <http://www.research.ibm.com/people/l/lipscomb/www-mpvr.html> (19 January 1997).

the display boundaries (walls), while the correct perspective and stereo projections of the environment are updated, ensuring the image moves with and surrounds him.[77]

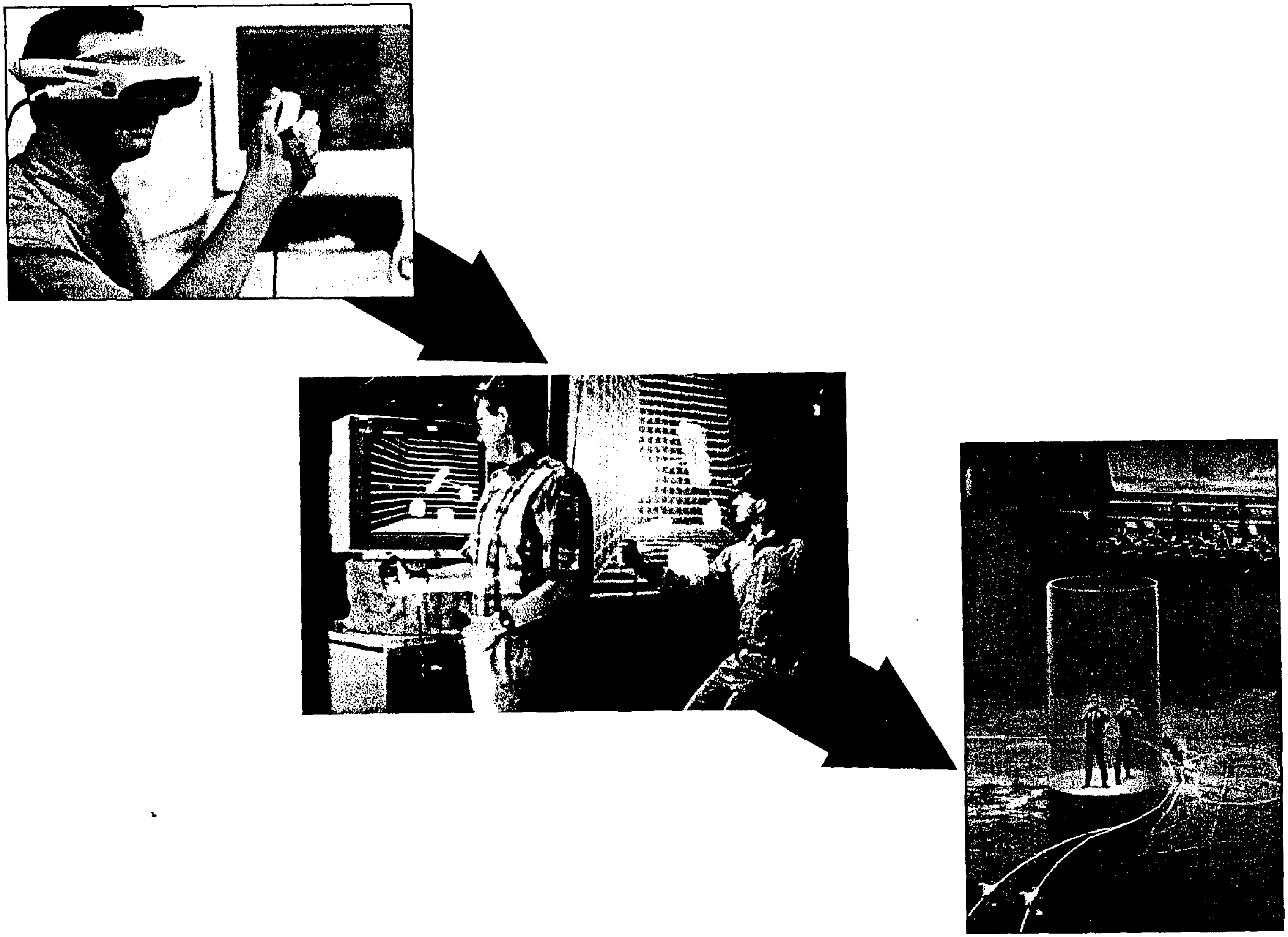
One of the central questions that emerges when one considers this wide spectrum of display means is "How is it possible for any domain controller to select between many competing images, displaying the resultant critical image to a viewer in less than a split second?" Perhaps some insight for prioritization of display scenes can be gained from examining the operations inside ABC network editing booths working Monday Night Football. Why is it so easy to envision and believe a technical coordinator inside a mobile van on Super Bowl Sunday manipulating and integrating over thirty screen shots and mobile van on Super Bowl Sunday manipulating and integrating over thirty screen shots multiple feeds in a split second and so hard for one to envision multisensory presentation fast-paced events in cyberspace on an operator's display screen.

Within the friendly zone of influence are valuable informational assets that DOD does not own but on which serve as important means of support. One could easily see where managing an information campaign in one's own zone of influence, similar to an army commander operating on his own familiar terrain, would be much less problematic than managing an operation extended through his entire zone of interest to the horizon beyond. Perhaps all a domain controller can do for the commander or operator is show him his own zone and what is going wrong, which may be enough for him to 'get a handle

---

[76] Kenneth Russell, Thad Starner, Alex Pentland, "Unencumbered Virtual Environments" (Cambridge, MA: MIT Media Lab, Perceptual Computing Group, Tech Report #305, presented at IJCAI Workshop on Entertainment and AI/Alife, undated), 1.

[77] University of Illinois at Chicago, Electronic Visualization Laboratory, CAVE Automatic Virtual Environment, HPCCV Publications, Issue 2 <http://www.ncsa.uiuc.edu/evl/html/CAVE.overview.html> (3 April 1996).



PHOTOS COURTESY OF IBM and AFMC

Figure 2-6 - A Spectrum of Display Means

on the situation.'[78] Within this zone, one must consider where to position the most valued objects. Are there any paradigms, which might help one think about *value* and how to protect it in cyberspace?

Locating and positioning resources. *Geoinformatics* is a new multidisciplinary approach to visualizing and positioning objects in information space, which is gaining interest among geographers. This process investigates things and events in cyberspace from spatial perspectives evolving from inside or outside traditional geographic studies.[79] For a geoinformatic approach to cyberspace to take hold, seemingly unrelated discplines like communications and geography will have to be combined for its most effective layout.

A new generation of cybergeographers have developed four ways of thinking of distance or 'metrics' that they hope will prove useful for operators in both the external or natural world and cyberspace:

- Physical Distance - the true distance between nodes in the real world
- Effective Distance - a functional definition of distance by time or cost
- Psychological Distance - a subjective measure of how close objects "feel"
- Integral Distance - where every link has unit length

The concept of effective distance would appear to be most applicable to locating and positioning resources in the information domain beyond the desktop. Objects in space might be scaled to their importance to us in time or cost. If cyberspace is a landscape, how does a geographer synthesize and unpack its 'rolling hills and dales?[80] Perhaps when one

---

[78] Bolt, interview.
[79] Swedish Royal Institute of Technology, Department of Geodesy and Photogrammetry, Welcome to the Division of Geoinformatics, 5 September 1996 <http://www.geomatics.kth.se/geomatics.html> (2 February 1997).
[80] Katsh, WWW.

unpacks it, they may want to use a special lens that enables only them to see these hills and dales and geo-location as a means of gaining relative advantage over other inhabitants. Or perhaps we build an intuitive universality into the topography that allows anyone (from an aborigine to a Wall Street executive) to readily deduce critical associations between objects. If military designers pursue such universality in cyberspace then they might display objects by familiar color association as red-hot balls. If military designers are pursuing relative advantage, the perhaps we need a filter mechanism which "colorizes" the entire scene for only us.

Since physical distance seems to have little or no meaning in the information domain, one must come up with a new way of representing how close or far apart two traditional "nodes" are. In the information domain, objects will not just feel close, they will *be* close. All of these metrics have their advantages for certain applications. However, none appear to be a true distance as intuitive as the one we think of in the everyday, external world. A context, which presents the intuition humans use in everyday life, is what information geographers, architects and toolmakers are currently striving for.[81] Perhaps the value of objects as in "amount of energy expended" or "threat" might be added to the definition of distance by time and cost.

Many of today's 3-D software applications allow users to dynamically alter their environment from within. These applications are building new expectations for users about dynamically repositioning objects in their surrounding environment. The next generation of military operators will need new architectural and art skills—a developed eye for the spatial--perhaps more than computer programming skills, especially if computer code is

[81] Maples, discussion.

imbedded in *infobs* described above as some scientists predict.[82] The military will also need to combine seemingly unrelated skills to map cyberspace--such as analysts from the National Imagery and Mapping Agency (NIMA) as well as DOD communicators—they will need to recruit more sculptors, painters, and those with an eye for the spatial than perhaps computer programmers and engineers.

It is important that any mapping system for cyberpsace preserve not only the essential features and objects of netwar or information warfare, but also some of the essential tasks. One of this critical tasks which has already emerged from "information defense" is the need to prioritize information resources to support defensive information warfare efforts. How and where to position what kinds of computers and related sensors, networks, databases, and so forth, may become as important as the question once was for the deployment of bombers and their support functions.[83] Researchers at the AFIWC are presently wrestling with the first part of this problem; testing methods for assessing and identifying the priority of specific information protect activities and operations using designators such as *essential, critical, significant, and trivial*.[84] The AFIWC presently has 53 sites in the USAF's Base Network Control Center (BNCC) system configured with their custom-made Automated Security Incident Measurement (ASIM) software protection tool. [85] They expect 104 sites to be configured by 1997.[86]

---

[82] Maples, discussion.
[83] Arquilla and Rondfeldt, 146.
[84] Roger D. Robinson, "Prioritizing Information Resources To Support Information Protect Operations," Trident Data Systems Research Paper for AFIWC/Computer Emergency Response Team Branch, December 1996, 3. This unpublished report is an attempt to conceptualize how the USAF might prioritize the defense of critical information systems and resources.
[85] Thatcher, interview.
[86] Ibid.

One should remember that the purpose of defensive information warfare is not to protect networks, or the stealing of data, but to preserve the commander's capabilities and prerogatives, or operational capability.[87] During an enemy information attack, commanders and operators should know upfront which resources are most valued: which ones need to be pulled into the core protection zone, which are to be kept at arm's length in the zone of influence, and which are to be closely monitored in the outer reaches of the zone of interest. Until recently, there has been no real national security or military effort to prioritize information resources or their protection. Presently the AFIWC's Computer Emergency Response Team (AFCERT) responds to 'whoever yells the loudest.'[88] Additionally, the USAF is still prioritizing incident response at the operator or tactical decisionmaking level. It could greatly benefit from a mechanism through which to view the 'whole information domain picture' as priority tradeoffs become more problematic given an ever-increasing attack rate.

Researchers at the University of Nottingham, in the UK, are working on an application for the visualization of document locations which might be helpful to the AFIWC and organizations like DISA charged with making decisions about the protection of information resources. The Nottingham approach is called VR-VIBE, a three-dimensional visualization and geo-location positioning tool initially developed for extensive document bibliographies.[89] In VR-VIBE, operators specify keywords that they wish to use to generate a visualization, and place these keywords in 3-D space.

[87] Robinson, interview.
[88] Thatcher, interview.
[89] Benford, Steve, Dave Snowdon, Chris Greenhalgh, Rob Ingram and Ian Knox, "VR-VIBE: A Virtual Environment for Co-operative Information Retrieval," Nottingham, UK: University of Nottingham, Department of Computer Science, 1995.

Documents are then displayed in the expansive space according to how relevant each document is to each of the keywords. The position of a document depends on the *relative importance* of each of the keywords to it; thus a document equally spaced between two keywords is equally relevant to both, while a document close to a particular keyword is relevant to that keyword only. *Absolute relevance* is depicted by the color of the document's representation; the more relevant the document, the brighter the color.

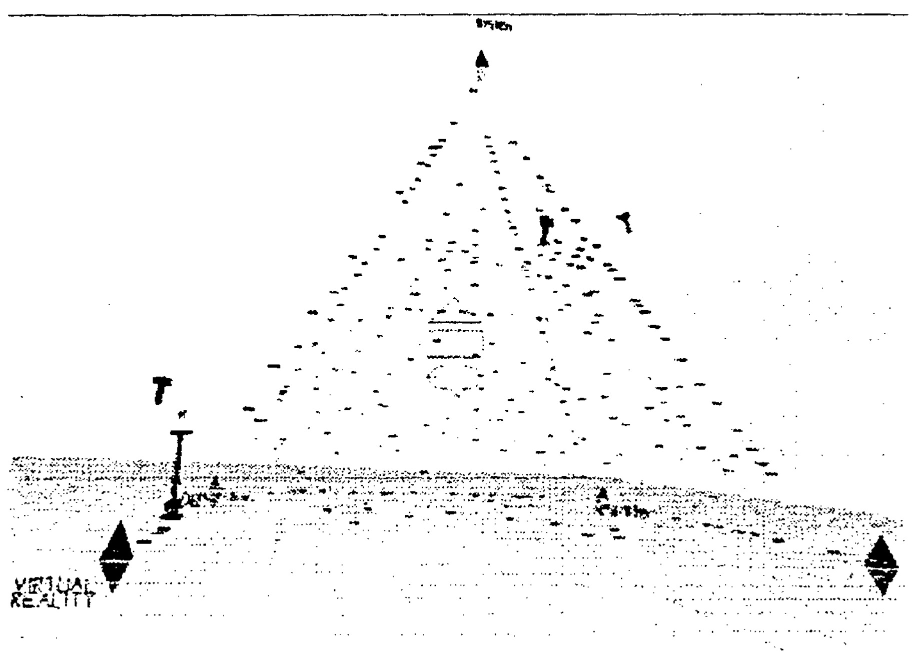


DIAGRAM COURTESY OF DAVE SNOWDON, UNIV OF NOTTINGHAM

Figure 2-7 - A VR-VIBE Visualization of a Large Bibliography

Figure 2-7 shows a sample VR-VIBE visualization of a bibliography containing 1581 entries and five keywords. Also visible are some other users browsing the information space which are represented as T-shapes. The position of the keywords are marked by octahedrons, with the text drawn alongside. Only documents with an absolute relevance greater than specified threshold are displayed, allowing the user to filter out less relevant documents. A 3-D scrollbar visible as the I-shape, with a sphere at the center bar of the I, allows the values of the relevance threshold to be varied. The triangular-rectangular-spherical icon in the middle of the document field represents the device used to move though the field which can be operated by joystick or mouse using immersive or standard computer means.

The VR-VIBE approach could have great utility for the AFWIC when they implement a method for prioritization of resources for netwar. Instead of keywords used by Nottingham researchers, one could easily substitute defensive IW *values* such as FAD, SMC, SV, and EAR explained in figure 2-8. Instead of documents floating in free space one might represent various US information resources ranging from DOD's classified message handling system to an USAF's F-16 logistics base. Time better spent on pattern recognition and anomaly detection would be saved and confusion generated from disparate interpretations about 'the defensive array' would be dissipated. Besides providing both commanders and operators a common, intuitive understanding of the cyberspace, operators would be given the flexibility to move critical assets back and forth between protection zones, even during a pitched battle. An imaginative defensive array might convince the enemy to go elsewhere, or one could use it to lure them into one's zone of influence, where they might be portrayed with greater fidelity, thereby exposing them to vicious counterattack.[90] At any rate, military operators, like today's new

[90] Wexelblat, interview.

generation of 3-D surfers, will be given the opportunity to reconstruct dynamically the domain from a position inside it—altering a previously static plane of activity.

As noted above, the good news for military leaders is that civilian researchers are already hard at work all over the world trying to build useful information space and environments.[91] Perhaps military efforts should be focused on the unique considerations, demands and requirements that warfare brings to constructed information spaces.[92] In this new information domain, traditional design principles must be reexamined, and new vocabularies invented to be consonant with not only new multisensory environments, but for the military's purposes must reflect attributes of campaigns. Therefore it must have features that can be integrated into planning with the other dimensions of warfare.

Force Activity Designator (FAD) – identifies the importance of a specific unit or program to the DOD mission. The FAD is derived from the precedence rating assigned by the Air Force
System Mission Contribution (SMC) - the unit commander or his designated representative identifies the contribution of each system to the unit's mission capability. The value ratings include Essential, Critical, Significant, and Trivial.
System Value (SV) - product of the unit's or program's FAD and the system mission contribution. System value indicates the relative importance of a specific automated information system to the DOD mission.
Exploitive Activity Rating (EAR) - an adversary may use a wide range of techniques to exploit USAF automated information systems. These techniques result in different actual and potential impacts on Air Force operations. This rating establishes the relative seriousness of specific techniques to USAF operations. The activity most seriously threatening the USAF (root intrusion) would be rated 10. The least threatening activity would be rated 1.
Incident Response Priority (IRP) – product of the system value and adversarial activity rating. The AFCERT, if forced to allocate resources, would consider the incident with the highest IRP.
FAD * SMC = SV **SV * EAR = IRP**

TABLE COURTESY OF ROGER ROBINSON, TRIDENT DATA SYSTEMS

Figure 2-8 - Potential Geo-Locational Values

[91] Andrews, interview.

CHAPTER III

EXPLORING THE INFORMATION DOMAIN

Challenges in Navigating Space and Time.

Portrayal, visualization, and topology are key variables in the exploration equation, but how can operators use new interfaces not to just read but *move through* and explore the new terrain described above? Ideally, today's researchers have concluded that they should be able to view, manipulate, and move through data as though in a separate multidimensional world, much the same as one moves on land, or perhaps more accurately, outerspace. Tomorrow's warfighters will almost certainly need navigational vehicles to explore new topologies and their corresponding spatial patterns. What will the 'dog sleds' of future explorers look like?

Navigational devices developed for cyberspace will no doubt influence its topology much the same as its topology will influence them. The relationship is iterative. Perhaps if the navigational means is capable and powerful enough, the landscape will be restructured to fit within the exploring vehicle's 'field of view,' similar to how data available on the Internet is now being restructured and tailored to fit within the World Wide Web (WWW) used to navigate it.[93]

If one can escape the standard land-locked networks for the freedom of innerspace, a paramount concern might be how to navigate a space, which appears to have no up or down. Does one navigate by object-visualization like in other domains? Explorers have traditionally traveled through one domain, yet have used others for

---

[92] Andrews, interview.
[93] Pesce, Kennard, and Parisi, WWW.

guidance. If naval vessels use the stars, land, and undersea features as reference points, will cybercraft use objects and information from other domains to operate? Perhaps domain controllers will have to *create* stars for use as reference points. Perhaps geographers and engineers will again unite to produce a 'you-are-here' application for the synthetic domain like the natural domain's Global Positioning System (GPS).

Confronted with these and other challenges in the exploration of the information domain, some researchers suggest that initial efforts should be focused on geographic content rather than navigation.[94] Yet, empirical research from the entertainment industry may prove the contrary. Steve Glenn, a former imagineer from Disney Corporation, described that when he was test-marketing a 3-D immersive game that brought the animated movie *Aladdin* to life, test participants became so enamored with the experience of navigating or 'flying' that the examining the highly detailed topography around them quickly became a secondary issue.[95] Disney then realized that time and energy spent on a high-fidelity, natural-looking topography and content was not worth the large monetary investment for animation. Clearly navigation in synthetic spaces is a revelatory experience in and of itself.

Given this country and our military's tradition of inquisitiveness and involvement in the exploration of the other domains, it is hard to believe that cyberspace will be consigned an unknown and undetermined junkyard under a convenient throughway, remaining unexplored. As people move about in vehicles in the external world, so they will want to wander about in vehicles in cyberspace. In the above characterization, the

[94] Bolt, interview.
[95] Edward P. O'Connell, "GDIP Trip Report to AIA Commander," San Antonio, Texas: AIA Command Section, February 1996, photocopy.

information domain is portrayed as multidimensional and therefore seems considerably different from the notions of physical space that many of us have.[96] This multidimensionality makes it very difficult to determine the overall structure of not just the WorldWide Web, but the broader information domain.[97] Anyone who has ever gotten lost inside a simple CAD program -- inverting themselves inside a solid object for example, might have special appreciation for the disorientation, frustration, and anger the first-time explorers of cyberspace are likely to feel. In many ways these pioneers will be shouldering all of the anxieties and fears of an entire generation.

Navigating the spatial realm however, will be the least of problems for future information operators. The biggest problem will be traversing x, y, z *plus* time. One might need to view time from an entirely different perspective. Time may not simply be a fixed and unchangeable facet or quality as it often is in the natural world.[98] In the military sector, operators make assumptions about time and structure norms and standards around these conceptions of time. Warfare itself has always employed time, invoked time, and carried expectations about time. Soldiers still "make up for lost time," and sometimes they march "double-time." Today's warfighter may be the first generation who actually works *with* time, whereas previously they merely worked *in* time and worked *through* time.[99] The military has long acted as if time is relative, an approach which will be advantageous for operations in cyberspace.

It is worth information operators time to reflect on this challenge: how to deal with its traversal in this new domain. Time in cyberspace pushes the present into the past and the

[96] Girardin, PDF format report, 9.
[97] Girardin, PDF format report, 9.
[98] Katsh, WWW. Katsh introduces the notion of *cybertime* to complement the notion of cyberspace.

past into the present in novel ways. Although people cannot know the future, they can continuously anticipate it and continually draw connections between the past, present and future. In this sense, one continuously shapes the present by interacting with a vision of the future, just as one shapes the present by interacting with a vision of the past. Again, computer communications allow us to now merge old bits with new bits.[100] We are starting to grasp that rather than being a limitation of cyberspace, time may offer us a unique *opportunity*. If these hypotheses were the case, information operators might navigate not only present time, but also future time, using it as a filter to determine what variable in the present isn't behaving the way they think it should.

Scientists tell us that every medium of communication has a bias toward either space or time that influences how it is used and what it is used for.[101] If the bias is in the direction of space, it supports communication from afar and fosters links among persons separated by distance. If it is biased toward time, it encourages the preservation of information over time. Operators will have to balance these two concerns as they navigate cyberspace, remembering that this will have many consequences for netwar.

The Potential for New 'Dog Sleds'

Moving beyond the computer. New interface devices can not only help the military solve problems of visualizing cyberspace and placement of assets and resources within it, they can also be used to help create navigational vehicles critical to its exploration. Engineers in the academic and commercial sectors are *presently* using

---

[99] Katsh, WWW.
[100] Katsh, WWW.
[101] Katsh, WWW.

immersive interfaces to move beyond the computer desktop, exploiting new possibilities for cyberspace exploration. The computer itself is in many ways a navigational vehicle, which changes our *perspective* of time. M. Ethan Katsh, a professor of cyberlaw at the University of Massachusetts, Amherst, alternately suggests that "our relatively brief experience with cyberspace indicates clearly that the computer is a space machine, negating physical distances and creating new spaces in which novel relationships and activities can occur."[102] Predictions like these make it more apparent why information technologists the world over are racing to find new methods for navigating cyberspace.[103] Throughout the ages, information has always been of little use if users could not find their way through it. Yet, like Admiral Peary they will need new dogsleds carrying the proper supplies to do this, mechanisms which are not just tied to the desktop, but which can be extended out into space—vehicles.

Importance of vehicles. In today's cyberspace represented by the Internet or WWW, users move *through it* by manipulating commercial navigators such as Netscape, powered by customized navigational tools such as Yahoo, Infoseek, and the like. In the future cyberspace already forming, the user or military operator will *be* the navigator, enclosed inside a physical or notional navigational vehicle. Military operators may want to build their own navigators for special types of netwar missions, powered by engines built to their specifications. One day, such vehicles might provide the military with a powerful means not only of conducting the necessary exploration of cyberspace, but also attaining critical netwar objectives.

---

[102] Katsh, WWW.

[103] Scientific American, videocassette.

A key question which will arise is *who* to build such devices and vehicle for? Questions like these are not so far off. The present debate about whether to utilize a national defense superstructure or a widespread militia approach is sure to have ramifications for whether swift craft are built for operators who fan out through cyberspace or whether more ostentatious chariots are built for commanders so they can move to 'the front' like General Patton at a moments notice. The AFIWC feels that ultimately national security protection mechanisms are heading toward decentralized implementation of the defensive information warfare mission, with centralized control or as they like to say 'correlation.'[104]

Observations from today and yesterday's pundits might lead one in the direction of designing cabs or vehicles for the tactical operator's use. Martin Libicki, predicts that information operations in the future will need to be decentralized, and most likely will follow the militia defense approach. Observations from Clausewitz about warfare in general seem to support this view: "As each type of terrain approaches its extreme it will, as we have observed elsewhere, tend to reduce a general's influence on events to the same degree to which it tends to emphasize the personal resources of the ranks, down to the private soldier."[105]

Standard heavy layered hierarchical command structures are already being obviated in the land, sea, and air and outerspace domains due to *perceived* time pressures.

---

[104] Thatcher, interview. AFIWC relates there are at least four key players in the information protect business worldwide with different 'pieces of turf:' the FEDCERT to protect the National Information Infrastructure (NII) headed by National Institute of Standards (NIST), Defense Information Systems Agency (DISA) charged with protecting the Department of Defense (DOD), CERT for the commercial sector headed by Carnegie-Mellon, and the Foreign International Response and Security Team (FIRST) which serves as the link to the international community's security concerns.
[105] Clausewitz, 349.

Why would one not think this trend will follow suit in the information domain where operators have already winced under *real* time pressures? Perhaps due to these emerging considerations, the future information operator will *be* a decisionmaker. In a decentralized netwar force, the sum total of individual successes may more decisive than the commander's topsight that connects them."[106] If this is the case, then it makes sense that these pioneers will need powerful tools that enable them to explore and fight—perhaps simultaneously—in a new frontier. The centralized versus decentralized control question will have great implications for not only what types of interface devices or vehicles are used, but at what level—tactical, operational, strategic—critical integration with other domains will occur.

New commercially-available network protection software is becoming more and more automated and proactive at sensing, detecting and even terminating attacks.[107] Yet there will be some critical elements of the domain that will be fluid and cannot be automated, and that will require expert repair or "man-in-the-loop" capability. Operators will need vehicles in which to cruise out and fix static or dynamic defenses.

Multisensory Control of Movement. Implicit in Gibson's original depiction of cyberspace, before being expropriated by the mainstream computer industry, was the use of *multi-sensory* devices for exploration or collaboration in the new domain. The term multi-sensory can be defined as one's use of the entire range of human senses and body movements to move themselves or other objects through a given space. Additionally, it involves and operators taking advantage of their own intuition and military skills (recognized through the ages). The famous psychologist Carl Jung discovered that

[106] Clausewitz, 349.

intuition was one of four ways people functioned along with feeling, thinking, and sensing. Psychologists are finding that not only does the environment (place)—described above—provide a critical nonverbal clue for human behavior, but also the mind, emotions, the body and the spirit.[108]

Researchers at enterprises as diverse as the University of Nottingham, UK and MuSE Technologies in Albuquerque, New Mexico are not only working on vehicles to overcome common problems of inconsistency and lost-in-cyberspace syndrome, but they are also working to change the 'division' of labor equation between the man and machine so that man is left with more time to work with metaphors, inferences, anomalies, and subliminals that provide deeper understanding and insight. Present-day computer users are still separated from the data they are exploring, with the machine acting as an intermediary.[109] Specifically, enterprises like MIT and MuSE have already proven that their intense study of not only human intuition, but the man-machine interface, can provide tremendous leverage for operators moving through future synthetic information spaces. The best navigation craft in this new domain will rely on human intuition and the senses. Like the new interface devices described above, new navigational vehicles will be unique not because they enable one to perform informational tasks faster than before, but because they change *how* one interacts with distant information and distant people.[110]

Future operators are going to need to reposition objects in cyberspace at *less* than a moment's notice. Researchers at MuSE, the University of Nottingham and BT have not only concluded that creative interfaces and tools give one significant capability to perform

---

[107] Thatcher, interview.
[108] Peterson, 9D.
[109] MuSE Tech, WWW.

these critical tasks, they are beginning to see that the whole body can act as a voice for emotion as well as navigation and communication. Advances in microprocessor performance, specialized graphics-rendering components, sound synthesis, speech recognition, synthetic voice production, stereo-optics, spatial position trackers, and display technologies have opened up new possibilities for interactive presentation of complex scientific and engineering data.[111] New immersive systems can permit the scientists and engineers to 'enter into,' and interact with, an artificial environment that consists of their data.[112] Such systems permit one's natural senses to be more fully utilized in exploring and understanding the information. The end result might be the creation of an interactive, *multidimensional* display environment, which can be explored by *multisensory* control of movement.

The universality of intuitive devices pertains not only to cross-cultural communication but also to communication by those with severe infirmities. Increasingly humans are using whatever sense they can to move themselves and objects through natural space so why should it be any different through cyberspace? Travis Roy, the tragically injured Boston College hockey player is able to move his wheelchair around by breathing through a straw-like apparatus. Wouldn't a commander want the mental power of a Stephen Hawking on his IW team, regardless of degree of infirmity?

Though visualization may be one the most important senses for mapping and geo-location of this new topography, other senses might exert a stronger influence when it comes to navigating or exploring this new information terrain. Visualization enables the

---

[110] Katsh, WWW.
[111] Ibid.
[112] MuSE Tech, WWW.

integration of vast amounts of information, but it is not the *only* sense as Dr. Arlan Andrews, one of the founders of MuSE Technologies explains:

> We can each scan the beautiful sunset over the beach, enjoying the natural scene, while listening to headphones, while being alert to a periscope or vessel in the ocean or a plane in the sky, or a beachcomber approaching us, *while* we feel the sea breeze, while we keep our balance and know the position of our bodies, and while we think about tomorrow's duties . . . all simultaneously and without interference.[113]

In various scenarios, the senses can be directly addressed; visualization is merely the most powerful one while one is awake. Standard visualization techniques and media offer: few interactive features (flat screen, keyboard, and mouse), information presentation that is almost exclusively visual, and severely limited real-time capabilities. Additionally, they do not support dynamic interactions with data that require new database computations (e.g., sorting, transformations, and correlation).[114] Sound may be more important in the exploration of cyberspace in some cases, while vibration, heat input, air flow, smells, pressure, may be used by operators to differentiate among clusters or classes of informational objects while navigating.[115]

Why 'multisensory presentation'? The human senses have evolved to provide human beings with the means to flourish in the four-dimensional world they inhabit (x,y,z plus time).[116] Yet, *how* information is presented to these senses is critical. In the 1950's John Von Neumann discovered there was a fundamental problem with computers or a bottleneck. The performance of computer systems was dedicated to the wire that connected memory to the processor. As computers have come more and more to resemble

[113] Dr. Arlan Andrews <aandrews@muse.musetech.com> "Re: Question." 24 October 1996. Personal e-mail, (24 October 1996).
[114] MuSE Tech, WWW.
[115] Andrews, e-mail.
[116] Andrews, e-mail

storage mechanisms, the processing element has now become similar to the human mind in a different kind of bottleneck. The problem today is not the computer, nor the operator, but *how* information is linked to the operator. If any human is 1,000 times faster than any computer ever built at processing data, then why does one remain so overwhelmed with data? If technologists can enhance an operator's perception then the promise of faster decision-making and movement via multi-sensory devices is enormous.

A Promising Vehicle. Though MuSE Technologies has designed a hovercraft for commercial examination of information spaces, and not specifically cyberspace, it might nonetheless prove useful for fighting netwars. Unschooled and unexperienced in the principles of infowar or netwar, MuSE engineers have examined the extensibility of the human body over time and space as a basis for constructing a cybercraft. The craft they designed is only three feet wide, with only enough room for a single operator an operator placed at the center of a notional transparent bubble. (From the outside the craft resembles the one driven by that famous extraterrestrial commuter *George Jetson* in Hanna-Barbera's animated cartoon of the late 1960's.) In this bubble, operators can put display windows anywhere they want—they are no longer limited to a 15 inch monitor.[117] Navigation aids on one transparent display wall of the craft might be used to give an operator a readout on his position relative to the core. An operator can answer his phone while looking at a calendar on the opposite display wall, while performing any number of other intuitive actions. When an operator turns from the calendar it simply vanishes from the wall of the craft.

[117] Maples. discussion.

One of the most critical capabilities MuSE engineers took into account when designing the hovercraft was the head motion of the pilot flying the craft.[118] Such head motion is critical to the mind's operation, and is how one perceives depth.[119] An operator in cyberspace will need to be able to move in one direction and look around in another much like pilots and drivers in the air and space domains. (One of the limitations of previous synthetic applications designed for 3-D commercial video games was that allegedly full-motion figures, embodying the user, could walk in one direction but were unable to turn their head to view space in another direction.) MIT researchers who previously worked on the SDMS project found that, for directness and efficiency sake, travel in synthetic space should have a few degrees of freedom--too many is madness.[120] Land vehicles may prove better analogs for cyberspace traversal in the short-term than air vehicles. Drivers of land vehicles point the front of their car with a steering wheel that acts as a critical vector or pointer guiding them through their journey. MuSE designers gave the craft a transparent outline in flight not only to enhance observation capability, but to provide this much-needed vector for an operator. Moreover, MIT and MuSE interface developers found that roll, pitch, and yaw capabilities of air vehicles might be too disorienting for initial use in cyberspace and that *hovering* right and left and up and down may be all that is necessary.[121]

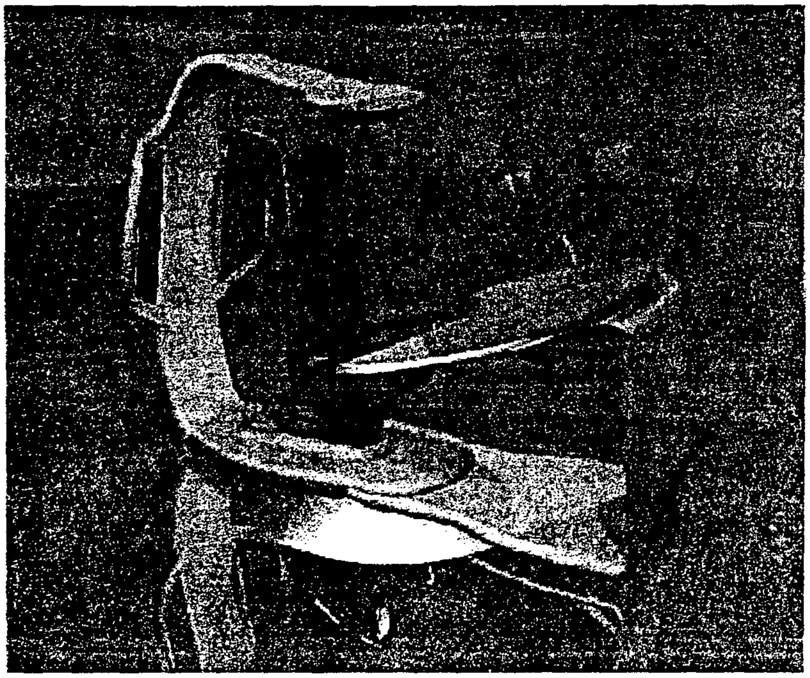
---

[118] Maples. discussion. Maples suggests that if a driver concentrates their gaze one foot above their right front headlight, after only five-ten seconds, they will begin to feel they are about to wreck the car because they are 'losing touch' with the world. Not being able to 'look around' hurts them in their ability to interpret and understand information.
[119] O'Connell, trip report.
[120] Bolt, interview.
[121] Maples. discussion.

The hovercraft operator will also be able to shrink the size of his vessel, and change its shape for closer examination of threatening objects such as time bombs and trap doors.[122] Unlike the air domain where the principal reason for changing the shape—or cross-section--of a craft is to hide from the enemy, in the information domain shape malleability can effect better, more insightful exploration of enemy objects and positions. For more standard examination of objects, the MuSE craft has a tether mechanism that can be extended by operators to allow them to attach to an object flying by.

It might be possible to customize MuSE vehicles for launch on specific national security missions in cyberspace. Shorter-range destroyers might be designed for use in the area of influence for detection of threats in the zone of influence. Longer-range cruisers might be launched to linger near enemy portals to pick-off targets of opportunity. Rather than mere computer workstations, more intuitive *docking* ports might be designed to launch and operate manned fleets out into the voids of cyberspace. Every second an operator wastes clicking on a button or icon with a standard mouse will break task concentration; breaks which could prove deadly in a fast-moving information campaign. New multisensory 'smart spaces' utilizing touch displays not only help overcome such limitations, but can also provide a stationary vector for the operator. BT engineers have just designed a private space for decisionmaking which could serve as a docking port for these vehicles. (See figure 3-1).

[122] Ryan and Federici, 6. A *time bomb* is similar to a logic bomb, except that this type of malicious object executes at a specific time rather than logic state. A *trap door* is a hidden software mechanism that permits systems protection mechanism to be circumvented.



DRAWING COURTESY OF BRITISH TELECOMMUNICATIONS

Figure 3-1 - BT's "Smart Desk": Potential Docking Port for New Vehicles

At present, researchers at the Air Force's Electronic Security Command (ESC) facilities at Hanscom AFB, Massachusetts, are experimenting with MuSE's hovercraft in the first phase of their research examining its benefits for simulating *airwar*.[123] They hope in phases II and III of their research to use a broader MuSE-designed multisensory environment to demonstrate in 3-D the movement of *live* aircraft and other objects in an airwar. During phase I, ESC engineers used the hovercraft merely as mechanism to examine simulated objects from this environment. As useful as the hovercraft already appear for merely simulating and exploring the dynamics of an airwar, and not as a

[123] Sommers, interview.

weapons systems itself, it might prove even more useful for *real-time* operations in a netwar.

Military Requirements for Exploration

Reflecting on the results of the *Day After* Exercises and Evident Surprise as well as Vice President Gore's broader national initiatives, an effective navigational vehicle should:

- Allow the operator to examine and navigate at the same time
- Serve as an interface to operators *outside* the domain
- Enable collaboration between operators *within* the domain

Need for simultaneous analysis and operation. Lessons from RAND's *Day After* have shown that analysis will need to be conducted by operators at various levels of connected information systems, interactively, *during* their operation.[124] The next generation of joint information operators, many of whom will not be from the traditional force execution community, will have to supplement their traditional 'examination' or 'communication' skill with interaction, navigation, and exploration skills. Present information warfare operators are already finding that up to 50-60% of their time is spent on research and only 5-10% is spent on analysis.[125]

Operators will have to perform more dynamic tasks like examining, navigating and perhaps attacking all at the same time. Because such tasks and roles are so intense, the modern-day USAF maintains separate aircraft and operators to perform them. Unmanned

[124] Robert H. Anderson and Anthony C. Hearn, An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: The Day After . . . in Cyberspace II, Santa Monica: RAND, National Defense Research Institute, 1996. ISBN: 0-8330-2452-3.

Aerial Vehicle (UAV) developers have realized for some time that--even in the relatively staid time environment of the air domain--pressures to attack targets almost from their first sensing are severe.

The use of such future navigational vehicles will make current information acquisition techniques and display seem like 'driving by rearview mirror.' These new ghost-like vehicles will need to be able to browse generalities or anomalies out in the unpredictable zone of interest, while exploring the details of the friendly zone of influence.[126] Operators of these vehicles ought to be able to enter cyberspace at any point in time, or push or pull the time lever back, *teleporting* themselves to T_1, T_2 or T_3 in cyberspace--wherever they think the problem is.[127] Using their tether, operators of these vehicles should be able to grab hold of objects whizzing by for close examination, or merely to enhance their own perspective. The tether might also be used to touch a neutral object or actor to see associative connections, or propagate histories about them. The operator now moves in the same orbit or direction as the object he has latched onto, perhaps leading him on a 'wild ride' out of their zone of influence and into an attacker's domain. In the not so distant future, one might have the option of not only *observing*, but also *embodying* any foreign object they choose out in an immense cyberspace.[128]

---

[125] Merritt, interview.

[126] Marcos Novak, "Liquid Architectures in Cyberspace," chap. in Cyberspace, ed. Michael Benedikt, (Cambridge: MIT Press, 1991), 239. Novak explains that in the natural domains two objects cannot occupy the same position at the same time. In cyberspace such a restriction is not strictly necessary. What seems most likely to occur is that entities will behave as "ghosts," passing through each other freely and interacting on the basis of a list of operations vaguely reminiscent of their natural world analogs.

[127] Benedikt, 171. Benedikt posits that a zone or sector of cyberspace may have a number of designated *transfer stations*, which transport users to other sectors very quickly, blindly, and without time proportionality to cyber-geographic distance.

[128] The author uses the term embodying to mean "taking on the characterisitics , attributes or perspective of a foreign object, for example in outerspace, becoming a satellite.

A navigational vehicle should also be able to project a grid to help with orientation. Perhaps operators might not just project a grid, but a mechanism that allows the operator to capture all resources in the immediate space of their vehicle in a given timeframe. This will not be just any passive grid, but a proactive and extensible net that allows one to collect, analyze and travel all at the same time. The hovercraft's unique "glass-bottom" would allow the operator to analyze the threats or objects caught in the net even as they move through cyberspace. One might almost imagine the enemy "catch of the day" trapped inside a net 'hanging from the craft.' To avoid collateral damage perhaps the net could be imbedded with code so that allied or neutral objects could wriggle away similar in a concept similar to dolphin-free nets fisherman currently use at sea (see figure 3-2). This would be "information on demand" taken to the nth degree.

Need for integrative function to other domains. One of the primary conclusions reached by participants in the *Evident Surprise* Exercise was that "CINC IW Operations must be synchronized with other [domain] operations, especially in conflict and war."[129] This conclusion, together with emergent fears that new means for conducting information warfare are being stovepiped, make the integrative issue a critical one for IW. It is not likely that the US will be fighting solely informational conflicts for some time, though in some instances third-world conflict over the infowaves has already commenced.[130] It is probably more likely that, in the near future, information campaigns will be conducted as part of larger war efforts featuring other warfare domains.

[129] US Atlantic Command, Joint Information Warfare Doctrine Development. 27 November 1996, briefing.

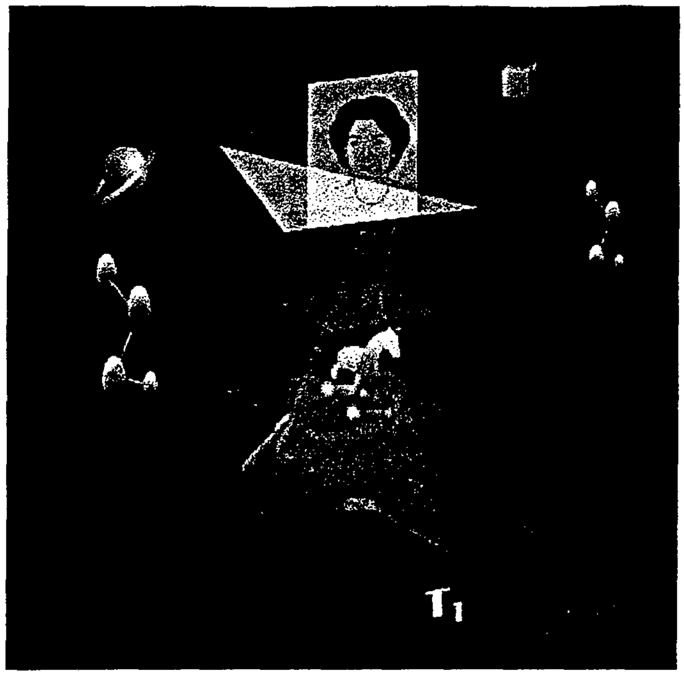


DIAGRAM COURTESY OF NWC GRAPHICS DEPT

Figure 3-2 - Moving From Browsing to *Catching*

Problems of natural-synthetic integration might be solved by simply adding display capabilities to each operator's navigational vehicle rather in contrast to today's approach of overlapping maps from three or four domains on a single screen for a commander. The key contributory function of a navigation vehicle would be its display panel, which could act as a window for operators passing information between two different domains, engaged by their concern over a common task or target. In the future, the panel might give full access for operators to move between the more external air, space, land, sea domains and the more internal information domain. The display panels would be the medium for decentralized control *and* execution; where the integrative function between forces in

[130] Hayden, briefing. General Hayden offers as evidence Mexican rebel leader Subcomandante Marcos's

different domains or components is performed not at the CINC or even the joint force commander's level, but at a much lower *operator-to-operator* level. This makes sense if one reflects that Clausewitz stated, "The peculiarities of terrain may be more important for the average soldier to understand than the commander himself.[131]

One can easily imagine a scenario where operators utilize an interface or display panel dedicated to allowing them to move between the more external land, sea, and outerspace domains and the more internal information domain. An operator in a destroyer might view a real-time downlinked video feed from an unmanned tactical aircraft (UTA) flying over an enemy computer facility, portrayed on the display wall (see figure 3-3). Such a capability would allow an operator to make a ready comparison between *internal* and *external* forces. Perhaps an information operator or commander would call off an attack if it looked like a UTA could better achieve the desired effect. An operator could run a 'what-if' simulation on the opposite sidewall of their craft, or pull in real-time feeds. One could also imagine the targeted computer's associative network portrayed on this wall.

retreat from government troops using 'info cover.' and Peru and Ecuador's short Internet War.
[131] Clausewitz. 349-350.

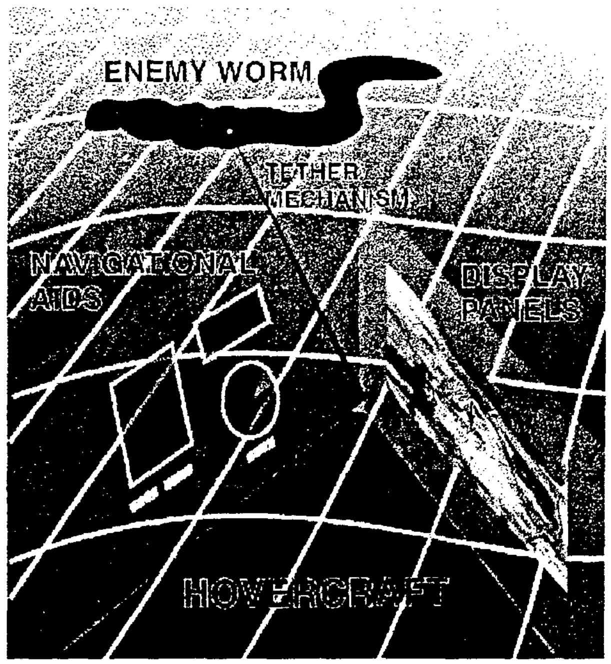


DIAGRAM COURTESY OF MuSE TECH, NWC GRAPHICS DEPT

Figure 3-3- Onboard Capability to Integrate with Other Domains

Need for collaboration within the domain. Perhaps even more critical than the need for information operators to integrate with operators from other domains is the need for effective *collaboration* between operators within the domain. The demand for collaboration seems to be superseding that of individuality among today's users of the Internet, surprising even the most prescient futurists. Mark Pesce, the creator of the virtual reality modeling language (VRML) recently predicted that someday soon cyberspace would hold the "galaxy of everything humanity has learned since we've invented writing, but instead of keeping it inside our brains, we keep it outside so other people can see it too." [132] In a similar vein, Vice President Al Gore recently issued the

[132] Miller, 8D. VRML is a 3-D technology which lets users navigate on line—not just up, down and sideways, but also from a changing perspective that lets them "zoom" in and out.

following challenge to the information technology and communications communities regarding the need for collaborative mechanisms:

> I would like you to take the critical next step [beyond visualization and computer graphics advances]. We need to move beyond web browsers into the world of *collaborative work.* The information needs of the government , industry, and public are becoming more complex and demanding new ways to link people across organizational, geographic and educational boundaries.[133]

Collaboration while working on a static project might be one thing, as shown in figure 2-1, but collaboration between two operators while navigating, during netwar, promises to be a much greater challenge. For all of the above discussion of the need for mechanisms built for single operators it is not improbable that in cyberspace as in the other warfighting domains, forces will continue to operate in teams—albeit smaller ones perhaps. More and more collaborative information systems are being used by the military in the natural domains as commanders and operators see the benefit of capturing all the mental energy available before making critical decisions.

Instead of handing tools to each other as described earlier in today's limited synthetic spaces, future operators will exchange perspectives between each other's craft while moving. This might be done using the tether mechanism extended downward to act as a link over which to pass critical protected information. One cybercruiser might view an enemy data trench from the highground above, pointing out potential obstacles and hazards to a comrade hovering below.

---

[133] Gershon and Brown, WWW.

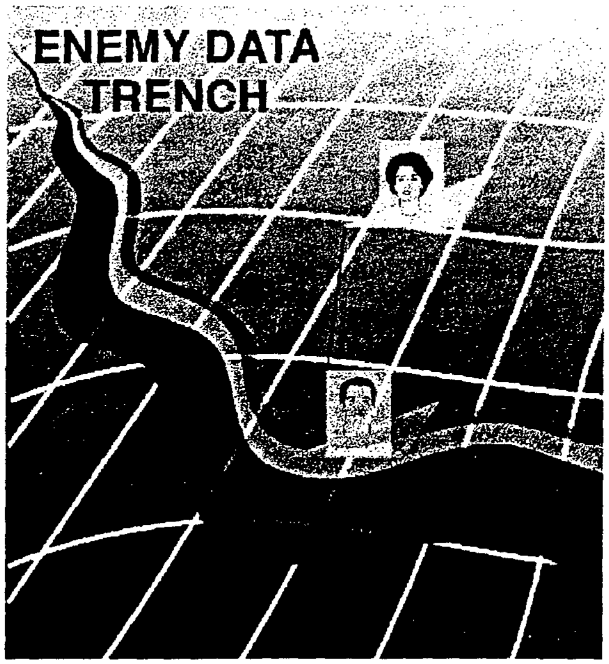


DIAGRAM COURTESY OF NWC GRAPHICS DEPT

Figure 3-4 - Exchanging Perspectives Within the Domain

The operator below could relay the details of the trench features as he snakes along its inner walls.

CHAPTER IV

GETTING INSIDE THE ENVIRONMENT

> . . . some blend of geographer, communications theorist, surfer, and machine will present new ways of writing the lines of force on the underknown world of cyberspace.[134]
>
> J. Morgan Reid

Commentary.

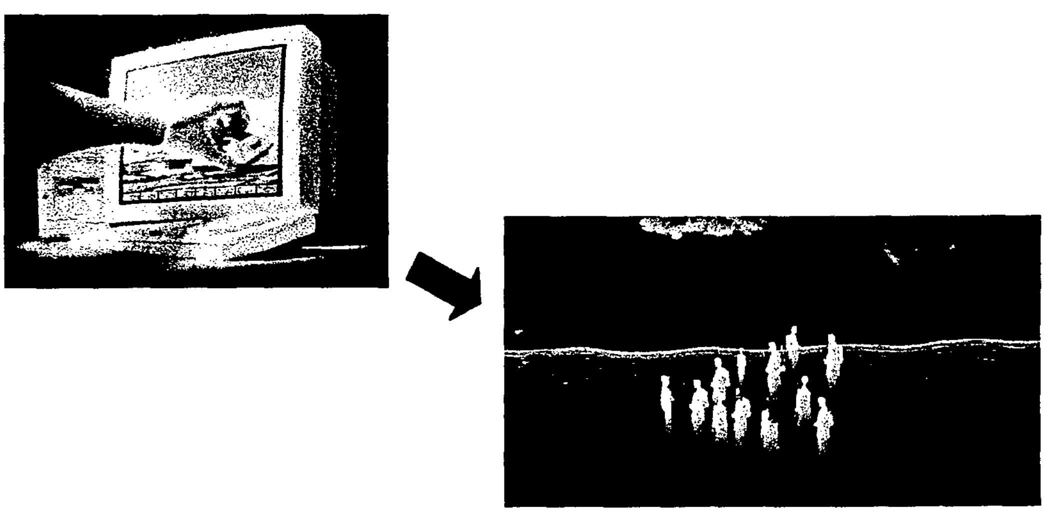
Research and analysis supports the contention that the information domain is a place, yet insights reveal that it is one unlike any other. Unlike the other natural domains, mankind is just on the brink of exploring the information domain. *One* of the most glaring problems is a lack of a mapping or coordinate system for the exploration of this space. Unfortunately, the expertise of military geographers has yet to be applied to this new frontier to facilitate exploration. Interfaces that might help are consigned to the 'back halls of the research labs' and remain either centered on modeling and simulating or the other warfighting domains. Conversely, the commercial sector, is already aggressively exploiting interface devices which not only assist in constructing and breathing life into cyberspace topography, but enable them to get *inside* the environment. The only way to find out what the military can do with new applications is to simply begin *exploring* the their possibilities *now*, for the purpose of staying ahead of our enemies. The military sector cannot afford to wait and hope that the commercial sector will let them know what happens.

Joint warfighters, are beginning to grasp the need for methapors or graphs to explain this new space. Research and analysis point outs that today's context and means

[134] Reid. 7.

of conducting information warfare are proving insufficient in capturing its true dynamics and challenges. 'Intuitive' devices that facilitate exploration of this new domain, vice separate navigation or examination functions look to be the most useful. The difficulty for the military is integrating science-fiction writers like Gibson's view with the network approach into a useful domain. Additionally, the military must consider the often radically different attitudes, expectations, and insights of a new generation of information warriors and balance these against broader truths about decision making and command and control.

A related problem confronting today's information warriors is how to portray this domain for the conduct of military operations. At present, this new information space seems to exist 'in the gray matter' of the minds of operators who are wielding traditional flat-screen interfaces merely to 'reach inside' it (see figure 4-1). Additionally, the military has no canvas or medium for discourse for cyberspace at present that is interoperable between all command levels. Though there has been limited discussion detailing the prioritized protection of information resources in this domain of space, there has been little



DIAGRAMS COURTESY OF SUPERSCAPE, AIA GRAPHICS DEPT

Figure 4-1 - "Reaching In" Versus "Operating from the Inside"

attempt to locate them spatially or temporally in a synthetic information domain.

New employment tensions can also be expected as the military gains understanding of the paradoxes and limitations of cyberspace. If this new environment turns out to reflect a greater time versus spatial influence, operators at lower levels might find themselves in the 'hot seat' of decision making. However, if history is an indicator, this decentralized approach may face problems when a transition in control--from the captains and majors currently dictating the priority for protection of service resources and responses--to senior national security officials takes place after the first nationwide incident.

Regardless of what approach the military chooses, the present flat-screen 'monitoring' approach from the outside will increasingly feel confining and constraining. Though the pressures and demands of the temporal dimension will prove shocking at first, human inquisitiveness will assuredly produce a dynamic environment where split-second reckoning between past lessons learned, present ROE, and future courses of action will ultimately be accommodated in some type of device or will be imbedded into a voxel of cyberspace.

Conclusions.

In the future, the key question for all sectors of society will no longer remain *access* to information sources. Technological advances described in this research and analysis are making this an insignificant factor. What promises to be a more important issue, is how to turn all of the data necessary to operate in the information domain into something more than a 'bit stream'—into something useful. Developers will have to turn this resultant information into knowledge of this new frontier, upon which an operator or commander can make decisions.

If a 'transition of command and control' takes place after an *Information Pearl Harbor*, the military sector must be ready to employ the very best mechanism for discourse which allows these new 'minders' a means to 1) frame and act upon decisions, and 2) integrate them with considerations from the other warfighting domains. At this point, the appropriate *presentation* of data in this domain—rather than access--will become the dominant concern. Factors such as how to conceptualize space and time, as well as protocols and interfaces, in ways that are appropriate for reflecting the dynamics of netwar, will prevail.

Navigation of this space will remain perhaps the most critical task for future operations. Research and analysis points out that, like the natural domains, devices that are intuitive and easy to use will be the most useful to operators, commanders and senior officials. An intuitive framework provides two benefits for integrating to other warfighting domains: from a broad perspective, a 'built-in' intuitiveness that parallels today's use of multiple senses in everyday activities, and from a narrower one, a tool in the navigation vehicle itself serves as an *interface* between inner and outerspace. The best navigational vehicles will not only allow one to traverse voluminous space and somewhat scarcer time, they will allow for much better quality interaction with*in* an information space than existing monitor, keyboard and mouse tools provide. If present day techniques allow us to connect pilots in live aircraft with simulators, hardware components, and laboratory testbeds, in the air domain, then one might expect architects could do the same with actors, and objects in the information domain.[135]

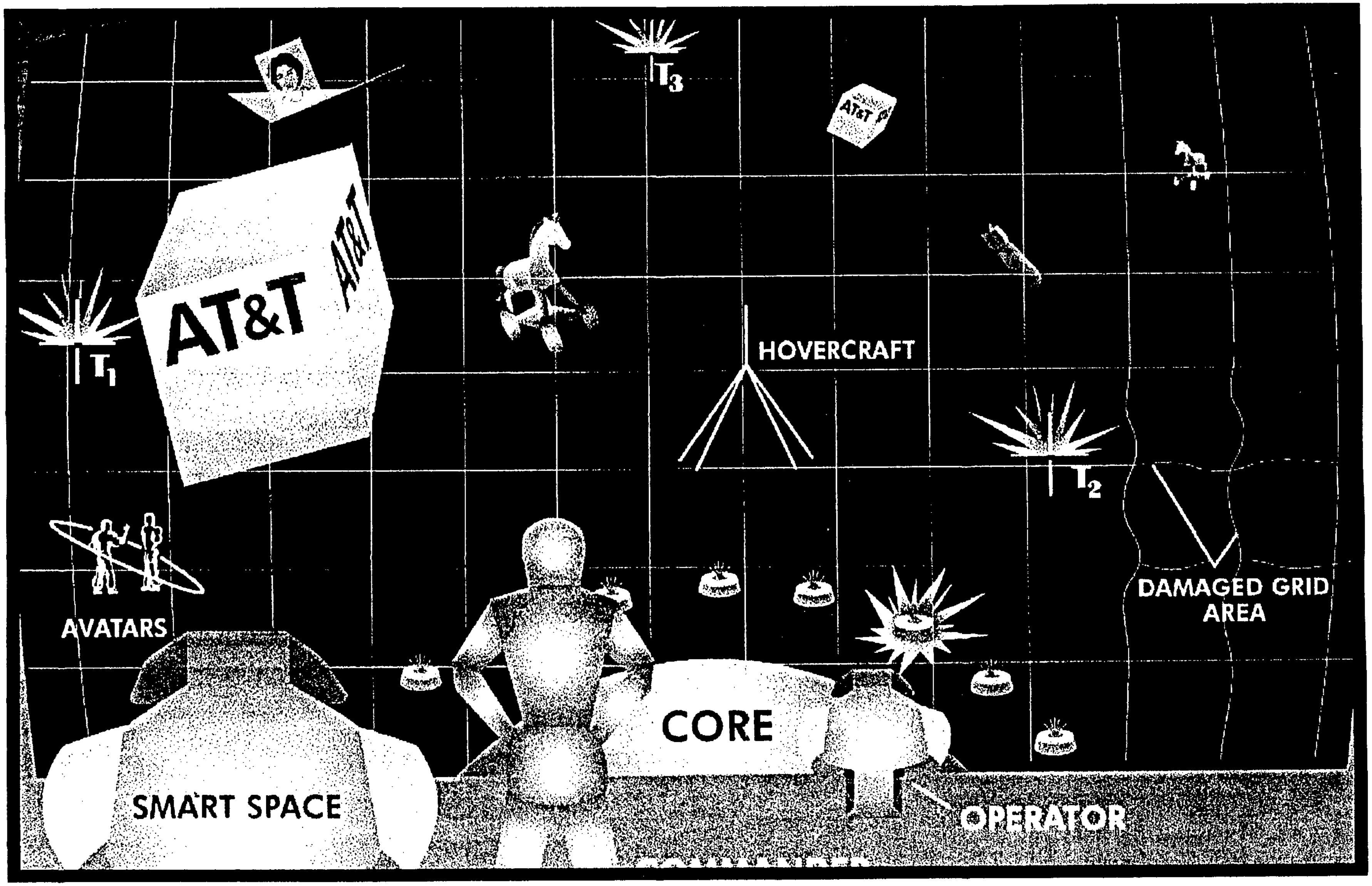
In scenarios where a CINC has been asked to provide visual results, reduce collateral damage, or display a situation to national security officials, they must have a good picture of what 'electronic force' will be required and how results will be verified. If the military does not have the requisite protocol, mapping and navigational devices, in place, they may inadvertently contribute to the CINC's perception that the use of information power may be prohibitively destructive. If netwar can't be integrated by some means, or reflect the intuitiveness of the more natural domains, the CINC won't accept the risks associated with its use, and the US and its allies may lose a valuable national security instrument.

Lending coherency to the 'information picture' will give joint force commanders a better grasp of the ebb and flow of the information battle, which will result in more flexibility for force application. Additionally, commanders and operators will be able to share their intuition with those in other spheres regardless of command structure. More importantly, they will have a medium for common discourse and become less reliant on disparate views of evolving situations over one-dimensional video or audio links. Patterns, relationships and perspectives between events will appear less chaotic thereby making 'cause and effect' more evident. They also have obvious benefits for the future operator who will be required to explore and fight *at the same time.*

When masses of electronic information are represented properly to existing human senses, better decisions can be made, and critical or peripheral problems not evident at

[135] Baker, 14.

first glance can be noticed. Operators can pick out trends, anomalies and patterns—so critical to decision making--from an 'information terrain,' regardless of where the data came from or what it means: moving forms indicate changes; constant shapes indicate static information; big things are close, and some things stop the motion of others (See figure 4-2). Unlike conflict in other domains, in information warfare, the practice field will *be* the battlefield or a very close approximation. Architects must begin to venture off the trodden path to paint metaphors and icons for *real-time* operations in a potentially more dynamic information domain.



DRAWING COURTESY OF NWC GRAPHICS DEPT
Figure 4-2 - An Environment "Rich in Content"

WORKS CITED

SOURCES: (ARTICLES, PAPERS, AND REPORTS - PUBLISHED)

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: RAND, National Defense Research Institute, 1996. ISBN: 0-8330-2452-3.

Massachusetts Institute of Technology. Virtual Environments in Command and Control for Ultra-High Definition Displays. RL-TR-96-120. Rome, NY: Rome Laboratory, July 1996.

Miller, Leslie. "Bringing A 3-D Experience to the Internet." USA Today, (9 January 1997): 8D.

MIT Media Lab, Personal Computing Section. Unencumbered Virtual Environments. Technical Report #305, IJCAI '95 Workshop on Entertainment and AI/Alife, Cambridge, MA: 1995.

Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson. Strategic Information Warfare: A New Face of War. Santa Monica: RAND, National Defense Research Institute, 1996. ISBN 0-8330-2352-7.

Peterson, Karen. "A Conscious Effort to Cultivate Intuition." USA Today, (26 November 1996): 9D.

Ryan, Julie. Offensive Information Warfare - A Concept Exploration. Center for Naval Analysis, Alexandria, VA: Jul 1994. Research Paper.

SOURCES: (ARTICLES, PAPERS, AND REPORTS - UNPUBLISHED)

Benford, Steve, Dave Snowdon, Chris Greenhalgh, Rob Ingram and Ian Knox. "VR-VIBE: A Virtual Environment for Co-operative Information Retrieval." Nottingham, UK: University of Nottingham, Department of Computer Science, 1995.

Ellis, Stephen R. "Presence of Mind . . . A Reaction to Thomas Sheridan's "Musings on Telepresence." Prepublication Draft, Moffett Field: NASA Ames Research Center, 1995.

O'Connell, Edward P. "GDIP Trip Report to AIA Commander." San Antonio, Texas: AIA Command Section, February 1996. Photocopied.

Rand. "The Day After Summary" 7 November 1996. Photocopied.

Reid, J. Morgan, "^Toward a Mapping of Cyberspace; Power, Creative Control, and Representation in the Post Fordist Nexus," Photocopied form Advanced Center for Spatial Analysis, University College, London, UK, 1996

Robinson, Roger D. "Prioritizing Information Resources To Support Information Protect Operations." Trident Data Systems Research Paper for AFIWC/Computer Emergency Response Team Branch. December 1996.

Russell, Kenneth, Thad Starner, and Alex Pentland. "Unencumbered Virtual Environments." Cambridge, MA: MIT Media Lab, Perceptual Computing Group, Tech Report #305, presented at IJCAI Workshop on Entertainment and AI/Alife. Undated.

US Air Force Information Warfare Center. Engineering Analysis Branch. "Automated Security Incident Measurement (ASIM)." December 1996. Working Paper.

US Air Force Information Warfare Center. Engineering Analysis Branch. December 1996. Working Paper.

SOURCES: (BOOKS)

Benedikt, Michael, "Cyberspace: First Steps." Chap. in Cyberspace: Some Proposals, ed. Michael Benedikt. Cambridge: MIT Press, 1991.

Card, Orson Scott. Ender's Game. New York: Tom Doherty Associates, 1991.

Gibson, William. Neuromancer. New York: Ace Books, 1984.

Johnson, Stuart E. and Martin Libicki. Dominant Battlespace Knowledge: The Winning Edge. Washington D.C: National University Press, October 1995.

Novak, Marcos. "Liquid Architectures in Cyberspace." Chap. in Cyberspace, ed. Michael Benedikt. Cambridge: MIT Press, 1991.

Peterson, John L. "Information Warfare: the Future." Chap. in Cyberwar: Security, Strategy, and Conflict in the Information Age, eds. Col. Alan D. Campen, USAF (Ret.), Douglas H. Dearth and R.Thomas Gooden. Springfield: AFCEA International Press, 1996.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Stephenson, Neal. Snow Crash. Bantam Books, 1992.

Von Clausewitz, Carl. On War. Edited by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1984.

SOURCES: (INTERNET)

AFCEA International Press 1996. CyberWar: Security, Strategy and Conflict in the Information Age - Introduction, eds. Col. Alan D. Campen, USAF (Ret.), Douglas H. Dearth and R. Thomas Gooden,<http://www.us.net/signal/AIP/ intro.html> lkd. <http://www.us.net/signal/> (19 December 1996).

Andrews, Arlan Dr. <aandrews@muse.musetech.com> "Re: Question." 24 October 1996. Personal e-mail. (24 October 1996.)

Andrews, Arlan Dr. <aandrews@muse.musetech.com> "Re: Work In-Progress." 13 November 1996. Personal e-mail. (13 November 1996.)

Elmer-Dewitt, Philip. "Welcome to Cyberspace: What Is It? Where Is It? When Can We Go?," Time Domestic, Special Issue, Spring 1995 Vol. 145, No 12, <http:pathfinder.com/@@zHGstAYA3U5xbeKK/time/magazine/domestic/1995/ special/tspecial.cover.htm> lkd. Martin Dodge,"Geography of Cyberspace: Some Other Useful References," 25 Nov 1996, <http://www.geog.ucl.ac.uk/casa/ martin/geography_of_cyberspace.html> (28 Nov 1996).

Ellis, Stephen. <silly@eos.arc.nasa.gov> "Re: Thesis Status." 3 January 1997. Personal e-mail. (3 January 1997.)

Gershon, Nahum and Judith Brown. Computer Graphics and Visualization in the Global Information Infrastructure: VP Gore Opening Statement, CG&A Special Report, Vol 16, No.2, March 1996, <http://www.computer.org/pubs/cg&a/report/g20060. htm> lkd. Martin Dodge, "Geography of Cyberspace: List of Documents," 25 November 1996, <http://www.cf.ac.uk/uwcc/cplan/martin/g...cyberspace/ geography_of_ cyberspace.html> (28 Nov 1996).

Girardin, Luc. Cyberspace Geography Visualization. PDF format report, Graduate Institute of International Studies, Geneva, 15 October 1995, <URL: http://heiwww.unige.ch/girardin/cgv/> lkd. Martin Dodge. "Geography of Cyberspace: Some Other Useful References." 25 November 1996. <http://www. cf.ac.uk/uwcc/cplan/martin/g...cyberspace/geography_of_cyberspace.html>(15 Dec 1996).

Girardin, Luc. Mapping the Virtual Geography of the World-Wide Web (WWW). Paper presented at Fifth Annual WWW Conference, Paris, France, 6-10 May 1996. <http://heiwww.unige.ch/girardin/cgv/www5/index.html> lkd. Martin Dodge,"Geography of Cyberspace: Some Other Useful References," 25 Nov 1996. <http://www.geog.ucl.ac.uk/casa/martin/geography_of_cyberspace.html> (28 Nov 1996).

Katsh, M. Ethan. Cybertime, Cyberspace and Cyberlaw (Article 1). <http://lii.cornell.edu/jol/katsh.htm> (19 November 1996).

IBM T.J. Watson Research Center, Yorktown Heights, NJ. Interactive Simulation in a Multi-Person Virtual World. <http://www.research.ibm.com/people/l/lipscomb/www-mpvr.html> (19 January 1997).

MuSE Technologies. MuSE (Multidimensional, User-Oriented Synthetic Environment): A Functionality-Based, Human-Computer Interface. <http://www.musetech.com/html/ijvr.html> (30 October 1996).

National Security Agency. Pointers to the Latest News on Telecommunications and Computer Technology. <http://192.13.244.99/ttn/5-1/pointers.html#HDR27> (9 April 1996).

Pesce, Mark D., Peter Kennard and Anthony S. Parisi. Cyberspace. (San Francisco: Labyrinth Group, undated), 1 <http://vag.vrml.org/www...concepts/pesce-www.html> lkd. Martin Dodge,"Geography of Cyberspace: Some Other Useful References," 25 Nov 1996, <http://www.geog.ucl.ac.uk/casa/martin/geography_of_cyberspace.html> (29 Nov 1996).

Plewe, Brandon, A Geography of Cyberspace: Is the Virtual World as Spatial as the Real World?, Geography 666, Spring 1995, University of Colorado, <http://www.geog.buffalo.edu%7Eplewe/cyberspace/> lkd. Martin Dodge,"Geography of Cyberspace: Some Other Useful References," 25 Nov 1996, <http://www.geog.ucl.ac.uk/casa/martin/ geography_of_cyberspace.html> (19 Nov 1996).

Schneider, Eric (eric@bash.cs.tamu.edu). "What is Cyberspace?" List of Frequently Asked Questions on Alt.cyberpunk, 18 October 1996, <http://bush.cs.tamu.edu...ch/alt.cp.fag.html#sec3> (28 Nov 1996).

Smith, Marcus. <marcus.smith@bt-sys.bt.co.uk> "Re: Question." 2 January 1997. Personal e-mail. (2 January 1997).

Swedish Royal Institute of Technology, Department of Geodesy and Photogrammetry. Welcome to the Division of Geoinformatics, 5 September 1996 <http://www.geomatics.kth.se/geomatics.html> (2 February 1997).

Takeyama, Masanao. Toward Cybergeography: A Proposal, <http://www.sfc.keio.ac...ography/proposal_e.html> (30 November 1996).

University of Illinois at Chicago, Electronic Visualization Laboratory. CAVE Automatic Virtual Environment, HPCCV Publications, Issue 2 <http://www.ncsa.uiuc.edu/ evl/html/CAVE.overview.html> (3 April 1996).

SOURCES: (INTERVIEWS)

Andrews, Arlan Dr., Vice President/Marketing, MuSE Technologies Incorporated. Interview by author, 6 December 1996, Albuquerque, New Mexico.

Bolt, Richard Dr., Senior Research Scientist/Program Manager. Interview by author, 3 December 1996, MIT Media Lab, Cambridge, Massachusetts.

Kelly, Lt Col Richard, Space Operations Officer. Interview by author, 8 January 1997, Naval War College, Newport, RI.

Maples, Creve Dr., Vice President/Operations, MuSE Technologies Incorporated. Discussion with author, 10 December 1996, Albuquerque, New Mexico.

Merritt, Larry, Technical Director, Air Force Information Warfare Center. Interview by author, 10 December 1996, Kelly AFB, San Antonio, Texas.

Robinson, Roger, Trident Data Systems, Development Engineer. Interview by author, 11 December 1996, Kelly AFB, San Antonio, Texas.

Smith, Marcus, British Telecommunications Development Engineer. Interview by author, 3 December 1996, MIT Media Lab, Cambridge, Massachusetts.

Sommer, Major Hal, Electronic Systems Center/XRPW. Interview by author, 27 December, 1996, Hanscom AFB, Massachusetts.

Thatcher, Major, Chief of Operations Branch, Air Force Computer Emergency Response Team (AFCERT). Interview by author, 11 December 1996, Kelly AFB, San Antonio, Texas.

Wexelblatt, Alan, Research Assistant, Intelligent Agents. Interview by author, 3 December 1996, Learning and Common Sense Section, MIT Media Lab, Cambridge, Massachusetts.

SOURCES: (MAGAZINES AND JOURNALS)

Alexander, David. "Information Warfare and the Digitised Battlefield." Military Technology Journal, (September 1995): 57-64.

Aldrich, Major Richard W. "The International Legal Implications of Information Warfare." Airpower Journal, (Fall 1996): 100.

Arquilla, John J. and David F. Ronfeldt. "Cyberwar Is Coming!" Comparative Strategy, 12, n. 2, (1993): 141-65.

Baker, Sue. "Cyber War," Air Force Materiel Command's Leading Edge Magazine, December 1996, 14.

Batty, Michael and Bob Barr. "The Electronic Frontier: Exploring and Mapping Cyberspace." Futures, 26(7) (1994): 699-712.

Gleick, James. "Just A Damn Minute." New York Times Magazine, 14 May 1995, 12.

Gray, Colin S. "The Continued Primacy of Geography." The National Interest, (Spring 1996): 247-259.

Libicki, Martin. "The Emerging Primacy of Information." The National Interest, (Spring 1996): 261-274.

Mann, Steven. "Chaos Theory and Strategic Thought." Parameters, (Autumn 1992): 54-68.

Thomas E. Ricks. "Information-Warfare Defense Is Urged." Wall Street Journal, 6 January 1997, B2.

Shackleton, Lieutenant Ernest H. "The Heart of the Antarctic," National Geographic Magazine: An Illustrated Monthly, Vol XX (1909): 972 - 991.

Strickland, Frank B. Jr., "It's Not About Mousetraps-Measuring the Value of Knowledge for Operators." Joint Force Quarterly, Autumn 1996, 90-99.

"The Death of Distance." Economist, 30 September 1995, 6-28.

SOURCES: (SPEECHES AND BRIEFINGS)

Fogelman, General Ronald R.. "Keynote Address." Author's handwritten notes from speech delivered at USAF Advanced Air And Space Symposium, Maxwell AFB, Montgomery, Ala., April 1996.

Fogelman, General Ronald R. "Strategic Vision and Core Competencies." Speech delivered at the Air Force Association Symposium, Los Angeles, CA, 18 October 1996.

Jones, Jeff. "Spatial Realities: Individuals, Community, and the Social Geographies of the Internet." Paper presented at the Annual Meeting of the Association of American Geographers, Charlotte, NC., 9-13 April 1996. Dept. of Geography, University of Kentucky.

Hayden, Major General Michael V. "Information Operations, Information Warfare and Intelligence." April 1996 Briefing.

O'Connell, Edward P. Exploiting the Virtual Advantage for USAF Information Operations. Briefing to AFCEA Symposium on Advanced Information Technology, San Antonio, TX: April 1996.

US Atlantic Command. Joint Information Warfare Doctrine Development. 27 November 1996. Briefing.

SOURCES: (US GOVERNMENT GUIDANCE, ORDERS, REGULATIONS)

Muolo, Major Michael J. AU-18: Space Handbook An Analyst's Guide - Volume Two. Maxwell AFB, Alabama: December 1993.

US Army Dept. FM 100-6: Information Operations. Washington: 12 April 1995, Working Draft.

US Joint Staff, J-7 Joint Doctrine Division, Joint Publication 1-02, Operational Plans and Interoperability. Washington.

US Naval War College. Joint Military Operations Department. Methods of Combat Force Employment. August 1996. Handout NWC 4099.

US President. Executive Order 13010. Critical Infrastructure Protection. (15 July 1996).

SOURCES: VIDEORECORDINGS

MIT Media Lab. Virtual Environments in Command and Control for Ultra-High Definition Displays - Pt. 1: Creation of Symbolic Information. Produced and directed by MIT Media Labs. 10 min. 1995. Videocassette.

Scientific American Frontiers. Inventing the Future. Episode #701. Produced and directed for GTE by Chedd-Angler Productions. 40 min. 23 October 1996. Videocassette.