UNITED STATES
NAVAL WAR COLLEGE
Newport, R.I.

WAGING INFORMATION WARFARE:
MAKING THE CONNECTION BETWEEN INFORMATION AND POWER IN A TRANSFORMED WORLD

by

MARK TEMPESTILLI
Commander, United States Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

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: Mark Tempestilli

12 November 1995

Paper directed by Captain D. Watson
Chairman, Joint Military Operations Department

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority: NA	
3. Declassification/Downgrading Schedule: NA	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: Joint Military Operations Department	
6. Office Symbol: 1C	**7. Address:** Naval War College, 686 Cushing Rd., Newport, RI 02841-5010
8. Title (Include Security Classification): Warfare INFORMATION WARFARE: MAKING THE CONNECTION BETWEEN INFORMATION AND POWER IN A TRANSFORMED WORLD (U)	
9. Personal Authors: MARK TEMPESTILLI, CDR, USN	
10.Type of Report: Final	**11. Date of Report:** 16 MAY 1995
12.Page Count: 20 (plus notes, appendices, and bibliography) (44)	
13.Supplementary Notation: A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department. 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.	
14. Ten key words that relate to your paper: INFORMATION WARFARE, INFORMATION SYSTEMS, REVOLUTION IN MILITARY AFFAIRS, RMA, EXPERT SYSTEMS, JOINT WARFARE, IW, C2W, COMMAND AND CONTROL WARFARE, COMPUTERS, TELECOMMUNICATIONS, C4I	

15.Abstract: This paper discusses the emerging ways, means, and ends of offensive Information Warfare (IW). IW is seen as being conducted in a distinctly unique dimension, however, inextricably linked to time, space, and physical force. The context of major geo-social transformation from the proliferation and convergence of powerful information technologies is shown as an underlying theme for change in joint military operations. The nature of IW is viewed as interwoven in a highly interactive geo-social-technical tapestry--including various layers of organized conflict ("war organisms"), represented by an overall system of functional subsystems (physical, mental, spirit). The relationships among physical force, information, and will are deemed essential to leveraging information for appropriate and useful operational effects. The nature of IW and the relationships among the functional subsytems are presented as creating potential for a new level of warfare synergy. Controlling an "information continuum" of information--knowledge--capability is seen as the key to generating information-based military power. New potential high value target sets are revealed that demand unique understanding and orientation--including a full development of IW beyond the current military interpretation as Command & Control Warfare (C2W). A comprehensive view of offensive IW is presented in terms of target development, weaponeering, military options, and organizing for action.

16.Distribution / Availability of Abstract: UNLIMITED	**Unclassified** X	**Same As Rpt**	**DTIC Users**
18.Abstract Security Classification: UNCLASSIFIED			
19.Name of Responsible Individual: Chairman, Joint Military Operations Department			
20.Telephone: (401) 841-3414/4120		**21.Office Symbol:** 1C	

ABSTRACT

This paper discusses the emerging ways, means, and ends of offensive Information Warfare (IW). IW is seen as being conducted in a distinctly unique dimension, however, inextricably linked to time, space, and physical force. The context of major geo-social transformation from the proliferation of powerful information technologies is shown as an underlying theme for change in joint military operations. The nature of IW is viewed as interwoven in a highly interactive geo-social-technical tapestry--including various layers of organized conflict ("war organisms"), represented by an overall system of functional subsystems (physical, mental, spirit). The relationships among physical force, information, and will are deemed essential to leveraging information for appropriate and useful operational effects. The nature of IW and the relationships among the functional subsystems are presented as creating potential for a new level of warfare synergy. Controlling an "information continuum" of information--knowledge--capability is seen as the key to generating information-based military power. New potential high value target sets are revealed that demand unique understanding and orientation--including a full development of IW beyond the current military interpretation of Command & Control Warfare (C2W). A comprehensive view of offensive IW is presented in terms of target development, weaponeering, military options, and organizing for action.

"In an important sense this world of ours is a new world, in which the unity of knowledge, the nature of human communities, the order of society, the order of ideas, the very notions of society and culture have changed and will not return to what they have been in the past... One thing that is new is the prevalence of newness, the changing scale and scope of change itself, so that the world alters as we walk in it... What is new [are] the techniques, among which and by which we live, multiply and ramify, so that the whole world is bound together by communication... The global quality of the world is new: our knowledge of and sympathy with remote and diverse peoples, our involvement with them in practical terms, and our commitment to them in terms of brotherhood... ...this is the world that we have come to live in. The very difficulties which it presents derive from a growth in understanding, in skill, in power. To assail the changes that have unmoored us from the past is futile... We need to recognize change and learn what resources we have."

- J. Robert Oppenheimer, 1955

WAGING INFORMATION WARFARE: MAKING THE CONNECTION BETWEEN INFORMATION AND POWER IN A TRANSFORMED WORLD

REACHING FOR THE ESSENTIAL CONNECTION

Information is about connections:

- connecting raw information to a worthwhile representation,
- connecting a sense to a perception and then to action,
- connecting a sender to a receiver,
- connecting many people to each other in organizations,
- connecting economic and cultural systems to an information basis,
- connecting neurons and a brain to form mental capacity,
- connecting an organism's mind to it's body and spirit,
- connecting machines and the people they simulate and assist,
- connecting technology and human response,

Ultimately it's about connecting information itself to power. It is this that is of central concern in all warfare and especially in Information Warfare. The environment of the Information Age and the very nature of information requires a holistic view--that there is a personal, human level to information, very much connected to the concept of Information Warfare. Information technology is therefore seen as a unique tool that is inseparable from the human social system as a whole. This is the constant in an era of global transformation. Because information speed, coverage, and capacity have greatly increased, geo-social-technical complexity is also multiplying--yielding both significant difficulties and opportunities in warfare. Through an understanding of how the nature of information is manifested in this context, the United States armed forces can wield extraordinary power--the essential connection in war, conflict resolution and deterrence.

THE INFORMATION AGE

Pervasive geo-social change is being driven by the explosive growth and convergence of related information technologies--computers, telecommunications, and other information systems. The global proliferation of these technologies and their applications have created a new "info-sphere."[1] Vice President Al Gore has said, "There is no longer any doubt that [computers and telecommunications networks] will reshape human civilization even more quickly and more thoroughly than did the printing press." Speaker of the House Newt Gingrich says that "the scale of change in technology will be so large that it is a change in kind." Economists and corporate management have embraced this transformation into what economic expert Peter Drucker calls the "knowledge-based society."[2] Expansion

of the infosphere is dissolving traditional boundaries, creating new complex relationships and interactivity.[3] The pace of change seems faster than ever before.[4]

Drucker's wisdom is particularly enlightening: "...[information] technology is important today precisely because it unites both the universe of doing and that of knowing, connects both the intellectual and the natural histories of man."[5] Furthermore, the technological trend is interwoven with other geo-social trends, ambitions and tendencies in a grand tapestry. The capability to process, deliver and access huge amounts of information[6] raises the average potential level of individual knowledge and number of available perspectives (whether computational or philosophical perspectives). Expansive, networked telecommunications provide heretofore uncommon potential to create new forums of extraordinary reach--to vastly multiply human interconnections.

These developments are enablers of any activity that is based on ideas and/or human "interconnectedness" and "relationalism."[7] This creates <u>both</u> enormous potential complexity <u>and</u> potential ability to derive simple, essential information and ideas from complex issues and sets of information. It is further vital to recognize that all these trends and potentials are meaningless except in a human context--that is, the conversion and application of information into ideas & knowledge, and then into utility or capability. The technologies, as breathtaking as they may sometimes appear, are only tools created by humans for potential human purposes--manifested in social activity, including conflict and warfare. This creates additional conditions for alterations in the fabric of social order. The increased potential both for complexity and derived simplicity or information essence, the global expansion of human interaction and knowledge, and their impact on the entire geo-social tapestry make the "Information Age" a fundamental transformation.

An extreme debate about whether this transformation is a true revolution or a stage of an evolutionary process may be counterproductive. We can see the Information Age as a revolution in geo-social intercourse scope and scale, or we can focus on the evolutionary effects--it doesn't matter--as long as we recognize it's roots and appreciate it's nature. The key issues for the United States military are that there is definite change going on, that it is generally global in scope and it affects all segments of the social system, that it therefore changes our operating environment and the character of some of our adversaries, and that it provides new capabilities--all of which apparently demand

new ways of approaching our business--that is: military power for national security. To deal with this highly significant set of changes--indeed, to capitalize on their very nature--requires new or adjusted frames of reference which allow a clearer understanding of the transformation in our own terms and provide the necessary vantage points for positive change, adaptation, and innovation to meet new challenges and fulfill new potential.

Meeting the distinct challenge of pervasive geo-social-technical change must be firmly founded in the fundamental requirement of providing military power for national security. Therefore, we must examine what the entire emerging geo-social-technical context means for national security and what it means to potential military power.

THE NATURE OF INFORMATION WARFARE and SYNERGY

Information is the capital of the mental & intellectual realm--a higher order human dimension. Machines may use information intensively, but only as they are designed to simulate an enlarged, accelerated, collectivized or otherwise enhanced, but fundamentally similar, human function. Human mental function attempts to convert raw information into knowledge and then capability in an "information continuum." Information-based machine systems are merely extensions of and assistants to this function.

All humans engaged in war--individually or collectively in organizations, unassisted or enhanced by machines--constitute what can be called and modeled as a "war organism." This human-based war organism consists of three basic functions and corresponding functional subsystems: physical, mental and spiritual. Table I, below, provides a simple expansion of this model.

Table I. "The War Organism" Model

Functional subsystem:	physical	mental	spiritual
"organic" concept:	skeleto-muscular	neurologic	psychologic+
war parallel:	mass, firepower	C2/C4I	will, cohesion, etc.

Information flows through, and is processed by, the mental subsystem--but the war organism is an holistic, interactive, interwoven system of subsystems. It exists on all levels--micro (unassisted individuals) to macro (technologically enhanced organizations)-

-which multiplies the potential for interactive complexity in larger and more collective organisms.

Clausewitz, who first reminds us that war is an act of force to compel the will of an enemy, says that "intellect is a clear, continuous vital contribution,"[8] inferring the connection between intellect and will. Sun Tzu spoke of subduing the adversary's will as "the acme of skill."[9] Indeed, Clausewitz recognizes the fundamental (even if increasingly macro) human nature of war as "nothing but a duel on a larger scale."[10] Furthermore, as the will, emotion and spirit reside together, Clausewitz recognized their relationship to an information continuum: "The step is always long," he states, "from cognition to volition, from knowledge to ability. The most powerful springs of action in men lie in his emotions." Sun Tzu wrote at great length about the informational impact on the will of the enemy. His work is traditionally interpreted as emphasizing intelligence and deception, however, in a larger sense it also describes the mental/intellectual clash that manifests the conflict of wills.

The enduring paradigm that war is a fundamentally human activity, given to complex interaction of two or more war organisms, to compel, subdue, or otherwise influence the will of the adversary is central, then, to the nature of IW. Physical warfare concentrates on compelling the enemy's will by diminishing his physical warmaking ability. Information Warfare not only bears on an adversary's will through influence in his mental/intellectual subsystems. If applied correctly it can have tremendous effects in the adversary's information-based infrastructure and strategic cohesion that sustains him, with consequent bearing on his will. Furthermore, the inherent non-lethal nature of pure IW makes new options available for for disrupting an adversary's entire interactive societal system by disabling key info-based subsystems. In this context, broad physical factors and broad mental & informational factors are synergized to create greater total power.

Thus, Information Warfare may be applied in three roles to control information and therefore gain power:

1) as an enabler or enhancer of own physical force, or by diminishing the adversary's physical force;
2) as direct attacks against adversary will; and
3) against adversary information not directly related to physical force, but with a definite bearing on the adversary's overall ability and/or will

The first role includes the traditional offensive warfare information loop of reconnaissance-surveillance-targeting-attack-assessment[11], traditional operation security (OPSEC), and most traditional forms of electronic warfare (EW). The second role includes traditional psychological operations (PSYOP). Traditional military deception falls within either of the first two roles. The third role is largely undeveloped, but ripe with potential in the Information Age.

FULLY DEVELOPED INFORMATION WARFARE

The "infosphere" is the dimensional link for the mental realm to the physical and spiritual realms. Information systems (even if temporarily independent of human interaction, as in a fire-and-forget weapon) are tools for work along the information continuum. Generating information-based power comes from controlling this continuum. The way to maximum power is information access and action to control it. Although thorough awareness of information is an enabler of power, the control of information can yield direct power over information-based systems, and powerful indirect leverage on the adversary organism. The control of information in any war organism, then, is a natural basis of generating higher military power through Information Warfare (IW).

CJCS Memorandum of Policy 30 merges OPSEC, EW, PSYOP, and deception under the relatively new discipline of Command and Control Warfare (C2W) and, based upon a classified DOD directive, states that "C2W is the military strategy that implements Information Warfare on the battlefield."[12] (Service policies have quickly fallen into line.) Two major drawbacks exist in this approach. First, it limits IW to the traditional battlefield. Secondly, it neglects the third role of IW --applications not directly related to physical force.

The infosphere has far surpassed traditional battlefield boundaries--physical as well as geo-political. Not only do new information-based targets within traditional objectives become relevant, but new ways of access also appear. The options to national security and military strategies are not limited to C2W. USAF Lieutenant Colonel Donald E. Ryan, Jr., in a recent article entitled, "Implications of Information-Based Warfare," correctly states:

> "We have reached a point where technology which supported combat has become a weapon in its own right. Again, under technological pressure, instruments of war are changing and leading to a concomitant need to change the methods of war."[13]

Since information is the only resource that can exist simultaneously in more than one place, and can be moved at the speed of light, it can transcend the time & space limits of physical force. This fact necessarily transforms the principles of concentration and economy of force. Operational tempo will be significantly altered, and not just in the physical realm, but in the synergistic application of all three IW roles. Whole new slants emerge for the definitions of depth and reach. A new information-based view of the indirect approach results. [Liddell Hart states: the "idea of the indirect approach is closely related to all problems of mind upon mind--the most influential factor in human history.[14]] Indeed, it is probable from a pure IW standpoint that the boundaries of rear, close, and deep areas disappear. Many IW targets will likely offer effects that transcend the functional levels of war. New strategic and operational options for deterrence, pre-emption, conflict, termination, and peace maintenance are created. IW includes C2W, but is much, much more.

A SAMPLE OF IW TARGET SETS

Examining potential targets opens a vista for new options in warfare, conflict resolution, and deterrence. IW targets appear available in most, if not all, information-based subsystems of any war organism. These information-based subsystems can be divided into four general categories; Table II illustrates:

Table II. Information-Based Subsystems/Targets[15]

Military/ Paramilitary	Organism Leadership/ Policymaking	Economic/ Commercial	Civil/ Utility
<----------C4I----------><---------telecomms---------->			
<----------transport---------->			
		<--------electricity--------->	
	state news media	private news media	
maintenance		finance	
supply & logistics		manufacturing	
training		oil	water
<----------individuals---------->			
netted formations platforms (note)	agencies	business units	forums

Note: Used here, "platforms" include those war organisms embedded in the larger military system, e.g. vehicles, combat systems, "smart" weapons & sensors, and countless information-action loops.

Table II is neither perfect nor comprehensive--it is generated mostly for illustrative purposes. There are likely to be many additional relevant subsystems.

Additionally, although they are listed under a predominant category, many of the subsystems may exist in multiple combinations, integrated vertically & horizontally--presenting numerous nodes of interaction which become potentially valuable targets in and of themselves. Those subsystems listed under the non-military categories also often have an undeniable relationship to the military. Many subsystems are in fact considered "dual use." Although many of these subsystems appear on the surface to be strategic in nature, depending upon the way information is applied (or attacked), they may actually have a direct link to the operational and tactical levels.

Electric power generation and distribution is a case in point for potentially vulnerable info-bases with multiple ramifications:

- power loss nation/theater-wide to diminish infrastructure for material war sustainment, or to bear upon the population's psyche is a strategic level action
- power loss in an area of operations could very directly affect the operational level
- disruption of power to a building or platform could be considered on the tactical level
- power loss that disrupts related C3 subsystems may affect activity at all three levels
- and so on...

Many of the info-based subsystems of Table II deserve discussion as relevant targets:

Finance. Includes banking, stock markets, trade & credit mechanisms. The Global Electronic Market Study found that 43 to 193 exchanges worldwide have electronic systems and 28 of those had been installed between 1988 and 91. Emerging economies are giving great emphasis to ground-up electronic market design and implementation.[16] Information subsystems exist in many segments of overall financial systems. Telecommunications is key to financial transfers. When the New York World Trade Center was bombed in February 1993, the neighboring Mercantile Exchange suffered electric power outage which resulted in 25% of the exchange's transactions going unprocessed the next day. "A full day's closure of the exchange would have cost the oil trading community $25 million and an extended shutdown would have been devastating."[17] One detailed study proposes a method for determining the value of attacking various financial systems. For example, Iran's foreign debt and imports-exports appear valuable, while China's entire financial system appears valuable.[18]

Electric Power Production and Distribution. "To ensure reliable service to customers, the status of a [typical] power system is monitored in an energy control

center through data acquisition and computing systems." In the control center an info-subsystem known as the Energy Management System (EMS) assists human dipatchers in monitoring, analysis, control, power distribution scheduling, etc. Advanced "knowledge-based" information systems for power system diagnosis and restoration offer additional capability.[19] Critical functions include intelligent alarm processing, electrical state security, and system diagnosis, performed either centrally or at substations, and decision and control for power restoration and remedial action. [The number of alarms in a typical power grid failure can be in the hundreds. Their number and combinations are nearly unmanageable without computer assistance or control.] Interestingly, among the many nations implementing these knowledge-based systems is the "hotspot" of the Federal Republic of Yugoslavia.[20]

Oil Production and Distribution. Knowledge-based expert information systems [henceforth "expert systems"] conduct flow control, production mixture control, pipeline leak detection, automated route changing, parcel tracking, and pipeline startup & shutdown sequencing. One corporation, Sd-scicon, has fielded over 300 expert supervisory control and data acquisition (SCADA) packages worldwide. Also, for example, distributive control systems (DCS) are well noted for roles in the production process by incorporating SCADA at distances over 60 miles and conducting such functions as supervising wells & valves, water injection, output flow of both oil and natural gas, emergency detection, separation of oil/water/gas, supervising tanker loading, and monitoring system temperature & pressure.[21]

Transportation Coordination & Control. Includes air traffic control (ATC), roadway traffic signals, railroad routing, and transportation system scheduling and manifesting. For example, regarding ATC, "the technologies for air traffic communication, navigation, surveillance and management are advancing at an unprecedented rate," including satellite-based surveillance, multi-national air-ground data links, and an international aeronautical telecommunication network (ATN). "Air traffic management will benefit from increasing automation. Flow management personnel will use improved aircraft positional information, large data bases, and sophisticated [computer] models to better predict congestion... for coping in real time," for both airborne and surface ATC.[22]

Water Treatment/Purification and Distribution. Expert systems are currently beginning development to assist management and control of these processes, although the

leap from the oil process should be short. Currently, expert systems are used to simulate the water process for diagnostic assistance and training. In diagnostics, all water treatment phases are touched---chemical addition, filtration, chlorination, etc.[23] Fresh water is a "fundamental" resource. Some recent American adversaries are very "water poor" and getting worse due to population growth, including Libya [drawing well over 300% of reusable supply], Iraq, and Iran.[24]

Supply/Manufactured Goods Distribution. Computer databases are key to output inventory and freight shipping management. The business world has found advanced information systems indispensible to responding "just-in-time" to both in-house process and customer needs.[25] Increasingly, transponders in shipping containers are tracked via satellite to aid distribution management. Potential is emerging for information system application to shipping fleet management including vehicle allocation, scheduling and routing.[26]

Telecommunications Systems. These include many advanced means of transmission for information sharing and delivery. In general, telecommunication systems can be viewed as a subsystem or enabler of a larger information-based system, or as the main system itself when considering the transmitted information as the primary product or objective. Telecommunication systems can vary widely in scale, scope, and type. A local area computer network (LAN), a telephone cellnet, and the infamous Internet are all variants. Various data handling schemes are employed with varying levels of central or distributive information routing control and information storage & servicing. They may employ various radio frequencies and/or various type cabling. Satellite, microwave, and fiber optic transmission paths are all growing. Worldwide infrastructure growth, a boom in international network privatization, a global trend toward service deregulation, and quantum leaps in communications technologies have converged in a telecommunications boom.[27]

News Media. Really a set of related organisms that are significantly enhanced and enabled by a wide range of advanced information technologies. The backbone of news media global reach is the global telecommunications infrastructure. As shown in Table II, the character of local news media may depend on who controls it, to what degree, and what their underlying news policy objectives are. The fundamental idea of controlling information to yield power is undeniably embodied in the concept of news media;

therefore, an adversary's relationship to news media and it's telecommunications backbone must be considered for potential impact on national security and military operations, if not as an outright target.

Information-Based Cycles.

- Critical development and sustaining cycles that are integrated into an adversary's organization are often enabled by information, use an information continuum, and function based on information technologies. Manufacturing & production, R-&-D & design, training, readiness, and materiel maintenance all exemplify this type of cycle. These may entail complex systems and complicated processes, but often it is relatively easy through familiarity, intelligence, or other foreknowledge to identify critical informational nodes and their technological basis.[28] As a very basic example, it has been widely reported that French export Exocet missiles were designed to include a secret "trap door" in the guidance program that would allow them to be disabled only by trusted agents. It would be highly desireable to similarly subvert an adversary's weapon systems during it's design and/or production cycle.

- Many critical operational-tactical cycles exist in aggregated or netted platforms and/or other information systems based on the organism model. The means and methods of generating a coordinated tasking order
is one example. The means and methods of coordinating targeting, positioning and launch of mobile theater ballistic missiles (TBM) is another. The sensor-through-shooter information loop is yet another. Similarly, these cycles may have vulnerabilities to information attack.

- Combining both perspectives leads to potential for actually subverting the development or preparation of these info-based op-tac organisms.

Platforms. Essentially, most platforms exist on the tactical level, although flagships and headquarters may be considered higher. Circumstances like coalescing into operational formations, or a platform delivering operational fires, may also raise their level. Information attacks on some info-dependent platforms may be feasible. Jane's guides abound with worldwide examples of combat vehicles and subsystems that exploit information technology to potential great advantage. Many may also be vulnerable as a result. These vehicles often employ drive- or fly-by-wire, and information intensive navigation & combat systems across the spectrum of dependence. Most include a data link

inter-platform networking scheme. Info-based vital subsystems, for example, of modern aircraft also include electronic fuel, thrust, inlet, and engine controls. Avionics averages nearly 40% of the cost of military aircraft.[29] The increasingly info-based automated design of cockpits (instruments, flight controls, etc.) offers potential vulnerability. A recent expert report indicates that pilots often don't recognize when the automated system has gone terribly awry.[30]

IW TARGETEERING

Potential information-based targets like those presented above require astute functional understanding for useful target development. The first requirement is to recognize what "type" of target/subsystem or combination of subsystems exist in the overall system. Basic target types are:

- an information system proper, normally based on tangible information technologies, with specific information components and an information handling design

- a platform with an embedded information subsystem, with or without immediate human interface

- information itself, i.e., that which flows through a tangible information system or otherwise affects information function of "info-consumers"[31]

- an info-consumer, i.e., a person or collective organization which receives information and uses it to form action; unless direct human connection occurs, some variety of tangible information system is involved

Tangible information systems and subsystems are of predominant interest, since they almost always provide a component of all other target types. Information systems can be further separated into four sub-classifications:

1) communications systems, including networking apparatus

2) simple data management, analysis, or display systems

3) "knowledge-based expert systems" which can judge inputs and make choices based on a database of programmed--and often complicated and unique--ways of interpreting information

4) "control systems" which control some physical process or function

These classifications imply different levels of development along the information continuum. Communications systems and simple data handling systems represent the most basic status in the continuum--unconverted information. Expert systems represent

information converted to knowledge. Control systems represent some level of conversion to capability for action. Generally speaking, the degree of dependence of an info-based function is inverse to the degree of development on the information continuum. Table III, below, represents this idea. (As will be shown later, dependence is a factor in the value of an information system as a potential target.)

Table III. Spectrum of System/Organism Dependence on Info Subsystem

fully independent <----------				fully dependent
direct human contact	simple info handling system	knowledge-based expert system	action-assist partial auto system	control system

Understanding target info-system design and characteristics is important to assessing the factors for target value and determination of useful candidacy. While a more detailed discussion is offered in Appendix A, technical comprehension of the candidate target should be acquired, to facilitate standard targeting judgements on relevance and usefulness of target candidacy, and the ability to access and attack it. This is known as mapping the info system "topography" (or infosphere topography in whole). Facets include:

Is the target info system...

- isolated or networked ?
- closed operating system or open ?
- serial processing or parallel ?
- local architecture or wide ?
- centralized function or distributed ?
- fixed or mobile ?
- electrically self-powered or externally fed power ?

[The most difficult target would probably be one which is isolated, closed operating system, parallel processed, local architecture, centralized function, mobile, and self-powered.]

Are critical information processing factors located in...

- hardware/circuitry ?
- the operating system ?
- the processing program(s) ?
- the data (while in transit, or stored in databases/files) ?
- the telecomms/network paths and nodes (including hubs, switches, and routers)?

Assessing target value, relevance of target candidacy, and priority of attack in the operational scheme also requires a comprehensive examination of value-added. This is a three step method:

1) First determine the value of the candidate target's information basis, including the following factors:

- Time-basis: Time-based components of value are often critical, including its useful endurance, sensitivity to timely delivery/presentation, and possible necessity for continuity of an info stream over time.

- Content: Does the information contain what the info-consumer needs for converting to useful knowledge?

- Quality: Components of information quality include timeliness, objectivity, usability, completeness, and accuracy.[32]

- Replacibility: Can the system restore the information, circumvent the disruption, "self-heal", draw on a backup? ...and how long would it take? Some distributive or parallel-processed systems have the capability to "self-heal" or reroute information as necessary.

- Dependence: As it refers to functional dependence. Already described in detail.

- Context: Can the information be recognized by the information consumer in it's appropriate context, i.e., in relation to other applicable information? Does it stand out from the torrent of irrelevant information?

2) Second, determine the relevance of the target to strategic & operational objectives and the overall operational scheme, including the following considerations:

- Value to the adversary info-consumer's strategic-operational scheme

- Value to own scheme & objectives, e.g. paths to centers of gravity

- "Time-match", i.e., for information of a transient nature, does it meet time-basis requirements, or would foregoing the information not matter over time?

3) Finally, determine accessibility of the info-based target. This returns logically to the necessary understanding of system topography, as discussed above, and--coupled with the weaponeering effort--determines target vulnerability to attack.

IW WEAPONEERING

In conjunction with the targeteering methodology, weapons must be matched to targets, delivery methods must be determined, and desired effects must be achieved. This can be represented by a seven step method:

1) Determine the type and level of "damage" desired, including these options:

- disrupt, deny
- degrade
- deceive, spoof
- accentuate, clarify (you may want to be sure the enemy has certain information for psychological purposes)
- shock
- destroy
- reconnoiter, surveil, collect

2) Determine level of covertness desired and risk if uncovered

3) Determine acceptable probability of "kill" or required probability/reliability of success

4) Analyze potential for desired or undesired information fallout, i.e. side effects such as cascading degradation in a system, or propagating through a network

5) Consider preferred method(s) of action/influence, including:

- software (remote entry point)
- software (local entry point; maybe delivered by covert agents or forces)
- electromagnetic/radio frequency (EM/RF)
- mechanical disruption (e.g. cut a cable)
- data injection
- data siphoning/extraction (total or selective)
- data reroute
- traditional hard kill (conventional weapons)
- unconventional hard kill (e.g. SOF direct action)
- traditional C2W (EW, PSYOP, MIJI, etc.)

6) Assess availability of weapon and delivery/application of resources

7) Match combinations of weapons, delivery methods, and timing to the target

Among all available IW weapons & methods of influence, software weapons offer extraordinary attack potential at low risk and low cost.[33] Discussing all the possibilities would fill a book. Appendix B provides background on some common software weapons like worms, viruses, logic bombs, etc. Software weapons can be tailored--multiple options and permutations are a strength of the medium--and can be stored long-term, or created "just-in-time." Although design and development of software can be highly labor intensive, it is nearly material resource-independent, especially when accomplished on desktop PCs.

One especially promising possibility is attack by expert systems or "intelligent agents" (sometimes called "knowbots"). A software agent is a program that can operate autonomously, carrying out tasks without direct human supervision. These could potentially patrol information systems and networks, searching for high value data, programs or systems, absorbing or altering information, deploying piggyback software weapons--even creating other agents, and--remarkably--"learning" and adapting to

unfamiliar target systems or target changes.[34] "Self-healing" distributive networks may actually negate the usefulness of conventional precision-guided munitions. Software agents may be ideal under these circumstances.

Two advanced EM/RF weapons also offer offensive IW promise. High Power Microwaves (HPM) "have the ability to enter structures via a slight crack or seam. They will even enter a metal container through apertures for transmission lines or sensor ports, and overload or short-circuit a single critical element of the target system, which is sufficient to render it useless." The main drawback of HPM weaponry is the amount of high energy and power density required, making currently available designs big and heavy.[35] DARPA has researched the development of "smart microwaves," with attributes that could damage a target, other than by high power. For example, high repetition rates or shaped pulsesmight be used.[36] The other technology that displays unique potential is Non-Nuclear Electromagnetic Pulse (NN-EMP). Anticipated EMP generators (deliverable by a variety of means) would create ultra wide band radiation with very fast rising times, on the order of 1 GHz or higher frequencies. EMP induces in any antenna, cable, connector, or conductor, a high voltage pulse that causes a disruptive surge, conceivably strong enough to destroy electronic components. Prototypes have been reported at defense labs, and cruise missile NN-EMP warheads are speculated have been speculated to exist.[37]

MILITARY MISSION OPTIONS

Information Warfare may be conducted in conjunction with traditional physical warfare or as a separate, stand-alone approach. In either case, several typical military options available for physical force could be used in IW, including:

- Blockade or Embargo: block the trans-border or pan-organization transfer of information, for example, electronic funds transfers

- Demonstration: show a belligerent that he is critically vulnerable to IW attack, e.g., take down his neighborhood power grid for a limited period

- Raid: conduct a precision IW attack against a specific information target or targets, e.g., decouple leadership communications from the organization

- Force Entry: conduct a coordinated multi-faceted IW attack against relevant information systems, e.g., choke transportation control, disrupt local media, turn off intrusion alarms, subvert supply distribution management, etc.

THE IW OPERATIONAL ENVIRONMENT

A key paradox will dominate the warfare environment in the Information Age: Either more centrally aggregated or more disseminated & dispersed information will be possible. As a result, complexity will significantly increase the possibilities in the following considerations as they apply to the entire geo-social context--that is, to adversary, neutral, and friendly organisms and methods:

1) control can be either more centralized or decentralized

2) capabilities can be more precisely customized singularly or en masse--not just in the production of materiel, but also in application

3) coordination can be conducted in time-based or info-based fashion, or in a complex combination

The interaction of these considerations combine to create a transformed operational context. A significant outgrowth is already apparent. Because "organisms" or organizations have less need to be physically aggregated, widely dispersed and diverse people will gain increased capability to coalesce around common ideas or goals. Paradoxically, small and closely located organizations will also be given unique access to diverse global information and the global scene. Both trans-national and sub-national organizations/organisms will be unusually empowered.[38]

Some trans-national entities already leveraging this new power include treaty organizations, non-governmental agencies, corporations, media organizations, environmental activists, terrorist organizations, and drug cartels. Sub-nationals include domestic political factions, insurgents, criminal groups, provincial and communal groups, and tribes. The interaction and synergism of these two concurrent, paradoxical trends could find sub-national groups banding together trans-nationally.[39] Global bureaus of non-governmental information agents already exist and are likely to proliferate. The increased complexity and speed of interaction breed spontaneity and a heightened level of activity, which in return feed back more complexity.[40] Army Chief of Staff General Gordon Sullivan describes one facet of this phenomenon as "hyperdiversity."[41] This condition poses a tremendous and fundamentally significant challenge to a nation-state's security apparatus.

Furthermore, not all corners of global civilization are advancing at the same rate. Today we see a "tri-sected world" containing societies essentially in the agrarian stage, industrial stage, or information-based stage of development, and some societies with

vicarious blends of elements of the stages.[42] Primarily agrarian societies have unique interests and newfound ability to incorporate some information-based capability and function for both domestic and global leverage. All this adds not only to the complexity of geo-social interaction, but also to the widely varying character of the field of conflict, and to the potential for strategic and operational friction.

The infosphere may be more or less developed in certain geographic areas, but it is enormous and advancing continuously. The phenomenon extends well beyond the "G7" nations. "In Hong Kong, 600 of the city's skyscrapers are already wired with fiber optics and rate as 'intelligent buildings.'...Singapore's leadership has vowed to make that country an 'intelligent island' by 2000."[43] India's public sector giant Indian Oil Corporation recently entered a partnership with IBM to address information technology requirements of oil refining and distribution.[44] AT&T does business in more than 200 countries, derives over 50% of its networked computing business outside the U.S., and has entered a joint venture to build an international telecomms network in Ukraine among many other overseas development projects.[45]

In 1991, the United Nations created the NGONET [NGO= non-governmental organizations] with specific concern for information networking in the southern hemisphere.[46] In Latin America, where only 7% of the population has access to a telephone, "the demand for communications has created the fastest growing cellular market in the world."[47] The Federal Republic of Yugoslavia has deployed advanced expert systems in management and control of its electric power grid.[48] A fiber optic network connecting major science research and cultural institutions is being developed in western Russia.[49] Oman's national oil terminal is described as "a windowless room [the 'spigot of the nation's prosperity'] filled with computers and pressure gauges that control the flow of Oman's crude oil through two floating buoys a mile offshore where tankers load."[50] In Blacksburg, Virginia--an "electronic village" sponsored by Bell Atlantic--a bank branch manager keeps in touch with a buddy in Iran "on-line."[51] During the UNOSOM II operation in Somalia, while American special forces pursued him, Aidid's scouts reported American movements via cellular phones.[52] Mexico's insurgent Zapatistas have routinely faxed open communiques from remote areas with noteworthy political effect.[53]

China has embarked on an amazing set of information development projects. Over the next decade, China intends to spend over $100 billion on deploying telecom equipment.[54]

China's Golden Bridge Project will eventually provide a network into 30 provinces, hundreds of cities, thousands of businesses, plus key utility systems such as the Daya Bay Nuclear Power Station. The Golden Customs Project will automate customs checks and international funds transactions to support foreign trade enterprise. The Golden Card Project will attempt to establish a national electronic money system with national credit and cash cards.[55] The Golden Enterprise Project will link commercial and industrial firms across the country, and provide business and industrial data for central and local government decisionmaking.[56] On 13 April 1995, it was announced that China's public telecommunications system joined the Internet.[57] China's explosive information technology growth is also observed in her military development. For example, China's upgraded Luda-class destroyers incorporate advanced information-based combat direction and fire control systems and new surface-to-surface missiles very similar to the Exocet.[58] A Chinese purchase of Israeli Elta EL/L-8300 SIGINT systems for airborne patrol and surveillance is pending.[59]

These salient cases convincingly portray the infosphere as globally pervasive and the geo-social-technical tapestry as woven evermore tightly, with more and faster interaction, and ever greater complexity.

ORIENTING FOR OFFENSIVE INFORMATION WARFARE

To achieve maximum military power and effect, IW efforts must be fully integrated into the strategic and operational schemes. IW actions and purposes must be sequenced, synchronized, and deconflicted with physical and psychological actions and purposes. Shares of the overall IW effort should be apportioned among the three IW roles, i.e.: as an enabler/enhancer of physical force; in direct attacks against adversary will; and against significant adversary information not directly related to the physical clash.

The CINC and his staff must undertake a comprehensive planning & preparation effort for anticipated IW. The J2 --assisted greatly by the J6-- must be the focal point for "information intelligence prep of the battlefield," wherein the definition of the battlefield has new meaning, and mapping the adversary's information topography assumes critical advance importance. J3 will necessarily take the lead on target selection and prioritization, assisted by the J2 and J6 in understanding the character of candidate targets. Finally, J3 will advance IW target recommendations to a Joint Targeting Board

(now dealing with physical and information attacks), which will integrate them into a composite Joint Integrated & Prioritized Target List (JIPTL) for coordination and deconfliction.

The national intelligence agencies must similarly undertake strategic-level information prep and mapping of the info topography, coordinating with CINCs' J2/JIC on collection objectives and resources, and sharing of IW-related intelligence. The national intelligence establishment should also seriously consider a strategic-level Integrated Information Operations Plan (IIOP).[60]

Service IW Activities should serve as the centers for warfighting expertise. The CINC and any pre-designated or standing CJTF staffs should have an officer dedicated solely to IW under the cognizance of J3. When necessary, the Service Activities should deploy Joint IW Augmentation Cells to these staffs. At minimum, primary subspecialties in IW should be established for these key personnel. Eventually, IW should become a designated warfare specialty/MOS in all the Services.

In the not-too-distant past, the U.S. armed forces embraced some previously non-traditional force options that have transformed warfare. The unique nature of airpower altered traditional military thinking about the limits of time and space, and provided powerful assymetric leverage against targets on all levels of war. The emergence of an extraordinary focus on special operations recognizes the unique nature of SOF to apply unusual methods of power, across the levels of war, often with effects disproportionate to the relatively small amount of effort used. The U.S. defense establishment should embrace a similarly holistic view of, and fully developed approach to, Information Warfare--going far beyond C2W. Both airpower and SOF provide useful doctrinal and functional insight into conducting IW.[61] It should be possible to analyze their respective approaches to the range of military operations and accrue a suitable start-up model for IW organization, training, and operational conduct.

The global commercial sector is fueling the development & proliferation of advanced info technologies, which in turn is fueling the geo-social transformation. Very fortunately, free world business--currently led by United States firms--constitute "partnership" opportunities for expertise & understanding of the infosphere, and to acquire and leverage cutting edge information technologies suitable to IW. Relevant access should be uniquely available to the U.S. armed forces at low technical risk and

relatively low cost. The Defense Department must fully capitalize on this phenomenon in development of, and orienting for, Information Warfare.

CONCLUSIONS: MAKING THE ESSENTIAL CONNECTION

In the throes of the Information Age, it is probable that we are reaching what Peter Drucker calls the second level of new knowledge or technology.[62] In the first level, technology is applied to improve existing processes and products. In the second level, technology is exploited to develop new and different processes and products. This is probably the case with Admiral Owens' "emerging system of systems" (ISR + C4I + PGMs).[63] Drucker's third level--by no means inevitable--is true innovation on a holistic level, based on a whole new way of thinking. U.S. Navy Commanders James FitzSimonds and Jan vanTol apply a similar approach to conceptualize Revolutions in Military Affairs (RMA). They posit that three preconditions are common to full realization of any RMA: technological development, doctrinal (or operational) innovation, and organizational adaptation.[64] "It is the synergistic effect of these three preconditions," they write, "that leads to an RMA." This correctly implies that RMA involves choices--that it is not a predestined occurrence, regardless of the technologic and surrounding social context, but ultimately dependent upon its embodied human interaction. Any vision of unique future capacity for military power through Information Warfare must absolutely consider that fundamental fact. Innovation will be dependent on human response, even more especially in the context of the fundamental geo-social-technical nature of IW. A "high tech - high touch" match must be achieved.[65] **Making the necessary connection between technology and human response in the complex and accelerated context of a transformed world will be the key to making the essential connection between information and possible revolutionary new military power for national security.**

NOTES

1. Alvin Toffler, The Third Wave (NY: Wm Morrow, 1980), p.184. This terminology has also been adopted in the "C4I For The Warrior" program, in a more limited way, i.e. as it relates to friendly military forces' information network.

2. Al Gore, "Infrastructure for the Global Village," Scientific American: The Computer In the 21st Century, Special Issue, 1995, p 156; Newt Gingrich, Unpublished text of speech on "Information Warfare" to AFCEA Conference, Arlington VA, 8 Feb 1995; Peter F. Drucker, Post-Capitalist Society (NY:Harper Collins, 1993).

3. The conventional economic wisdom is represented in the following passage from Karen Wright, "The Road to the Global Village," Scientific American, Mar 1990, p 94:

> "...the information economy is erasing another classic landmark: the national border. 'The absolute imperative of the information age is the need to establish a global economy,' says Penzias of Bell Labs [Arno A. Penzias, vice president of research at the time]. 'If you go to a party and someone says, 'What's your globalization strategy?' and you say, 'What's that?' you become invisible.'"

Additionally, in a speech delivered to the Commandant and senior officers of the US Marine Corps on 20 Oct 1994, Mr. William Van Dusen Wishard, President of World Trends Research, said:

> "Communication technologies are zapping all the artificial boundaries we've erected. For centuries, national, cultural and ethnic boundaries helped define a person or a group. Now those boundaries are falling, and they no longer constitute the outer limits of a people's identity. While cultural and national groupings will continue to exist, they will no longer form a relevant psychological boundary." (Van Dusen Wishard, "A New Frame of Reference," Vital Speeches, 15 Dec 1994, p 155.)

4. Consider: The "Agricultural Revolution" took 475,000 years from the dawn of man, the "Industrial Revolution" followed in another 25,000 years, the "Information Revolution" has taken a mere 250 years since. Strictly speaking about information, note that 50,000 years after man began to speak he invented writing, 5,000 years after he began to write he invented printing, 500 years after the first printed book he invented the computer, less than 50 years after the first computer we are in the throes of a new transformation. Less than 20 years ago, there were only 50,000 computers. Today, the industry sells 50,000 computers in one day. {see Charles R. Walker [Director, The Technology Project, Yale Univ.], Modern Technology and Civilization (NY: McGraw-Hill, 1962), p 331; Raymond W. Smith [Chmn & CEO, Bell Atlantic], "The Global Interactive Human Network," Vital Speeches, 1 Sept 1993; Bert C. Roberts [Chmn & CEO, MCI], "Information Highways Delivering and Shaping," Vital Speeches, 1 Feb 1994; and Charles R. Walker, Technology, Industry, and Man - the age of acceleration, (NY: McGraw-Hill, 1968), pp 1-12.}

5. Peter F. Drucker, Technology, Management, & Society (NY: Harper & Row, 1970), p 190.

6. Consider: A laptop computer today, costing less than $2000, is equivalent to the supercomputer of 20 years ago, costing millions of dollars, filling a space the size of six refrigerators and requiring four people to operate ["PC Power Surge," The Reporter Dispatch, (Yorktown Heights, NY: Gannett Suburban Newspapers, 10 May 1995), p A1]; The Internet is comprised of over 2 million host computers world-wide--ten times more than only five years ago [M.Mitchell Waldrop, "The Seeds of the Internet Boom," Science, 12 Aug 1994, pp 880-881].

7. These are my own words. "Interconnectedness" describes a state of complex connections, implying complex human interactivity as a significant result. "Relationalism" describes methods and means of relating myriad, and often disparate, information and ideas to each another in multiplicative combinations, creating many new human perspectives--it is derived from the notion of "relational" databases, storehouses of information that are purposefully related in various ways.

8. Clausewitz, Carl von, On War, Howard & Paret edition (NJ: Princeton Univ. Press, 1976), p 110.

9. Sun Tzu, The Art of War, S.B. Griffith, trans., (London: Oxford U. Press, 1971), p 77.

10. Clausewitz, p 75.

11. Advanced sensors, precision-guided weapons, C4I and their respective methods as they apply to diminishing adversary physical force are variations on this theme. JCS Vice Chairman, Admiral Bill Owens has articulated a vision of this particular category, most recently and with greatest detail in "The Emerging System of Systems," Naval Institute Proceedings, May 95, pp 35-9.

12. U.S. Joint Chiefs of Staff (Chairman), Command and Control Warfare. Memorandum of Policy No. 30, 1st Revision (CJCS MOP 30), (Washington, DC: 8 Mar 1993), p 3.

13. Donald E. Ryan, Jr., "Implications of Information-Based Warfare," Joint Force Quarterly, Autumn/Winter 1994-95, p 114.

14. B.H. Liddell Hart, Strategy: The Indirect Approach, (NY: Praeger, 1949), pp 18-19.

15. Two related views on target sets can be derived from the "five rings" model proposed by Colonel John Warden [enemy command, essential production, transportation network, the population, the fielded military forces], or the "squared" Clausewitzian trinity proposed by Professor Michael Handel [the people, the military, the government, the economy & technology]. Handel, Michael I, "Clausewitz in the Age of Technology," in Handel, ed., Clausewitz and Modern Strategy, (London: Frank Cass, 1986); Warden, John A., III, "Employing Air Power in the Twenty-first Century," in Shultz & Pfaltzgraff, eds., The Future of Air Power in the Aftermath of the Gulf War, (Maxwell AFB, AL: July 1992).

16. Smith, Carrie R., "Emerging markets ride the electronic wave," Wall Street & Technology, Apr 1994, p 38.

17. H.D. Arnold, et al, "Targeting Financial Systems as Centers of Gravity," Defense Analysis, Aug 1994, p 186.

18. Ibid. pp 183-4.

19. Chen-Ching Liu, "Knowledge-Based Systems in Electric Power Systems," Proceedings of the IEEE, May 1992, p 659.

20. Germond & Niebur, "Survey of Knowledg-Based Systems in Power Systems: Europe," Proceedings of the IEEE, May 1992, pp 737-740.

21. Mike Spear, "SCADA takes control of cross-country oil flows," Process Engineering, Jan 1992; and "Controlling oil flow on-shore," Process Engineering, 22 Mar 1992.

22. Bruce D. Nordwall, "Standards Main Hurdle to New ATC Technologies," Aviation Week & Space Technology, 16 May 1994, pp 46-47.

23. Collins, Catlin & Ilges, "Expert System Assists Operators," American Water Works Association Journal, Dec 1994, p 18.

24. Peter H. Gleick, "Water and Conflict: Fresh Water Resources and International Security," International Security, Summer 1993.

25. Michael Finley, "Making It Just in Time," Beyond Computing, Mar 1995, pp 49-50.

26. Victor Sandoval, "Computers, telematics, and road freight management," Impact, v.41, no.2, 1991.

27. For detailed background see [in reference to attached bibliography]: Ackerman; Braunberg; Cerf; Dertouzos; Gilder; Gore, "Infrastructure for the Global Village."; G.T. Global Financial Services report; Jackson; "Overview of AT&T's global presence: August 1994."; Soon; Waldrop, "The Seeds of the Internet Boom."

28. A few representative examples are mentioned in: Julie Ryan, Offensive Information Warfare--A Concept Exploration, CIM 361, (Alexandria, VA: Center for Naval Analyses, Jul 1994); and William B. Scott, "Information Warfare Demands New Approach," Aviation Week & Space Technology, 13 Mar 1995.

29. Bruce D. Nordwall, "Avionics Market to Improve in '96," Aviation Week & Space Technology, 13 Mar 1995, p 81.

30. David Hughes, "Accidents Direct Focus on Cockpit Automation," Aviation Week & Space Technology, 30 Jan 1995.

31. In information processing, information exists in three basic forms--raw input, in-process, and processed output--with only one desired exception. Unlike computers and their peripheral subsystems which exist exclusively to order, manipulate, relate, combine or calculate information, pure telecommunications systems strive to transmit information with no alteration from input to output. Additionally, unlike information systems, platforms, or info-users--which constitute variations of war/info organisms--the information itself is fundamentally

different. Information alone does not achieve action without conversion by an organism to capability and applied will to act--even if the decision to act is pre-programmed into the info system.

32. Illustrative variations and descriptions of information quality include: U.S. Navy Dept, Naval Command and Control, Draft NDP 6, (Norfolk, VA: Naval Doctrine Command, Dec 1994), p 33; Joint Chiefs of Staff, Doctrine for Intelligence Support to Joint Operations, Joint Pub 2-0, (Washington, DC: 12 Oct 1993), p IV-20; Tom Valovic, "Quality of Information--Part II," Telecommunications, Jan 1995, p 8.

33. Coherent discussions of development and delivery concepts for software weapons are found in: Peter C. Emmett, "Software Warfare--The Militarization of Logic," Joint Force Quarterly, Summer 1994, & "Software Warfare: The Emerging Future," The RUSI Journal, Dec 1992; and Thomas W. Madron, "Dealing with Worms and Viruses," in Network Security for the 90's, (NY: John Wiley & Sons, 1992).

34. M. Mitchell Waldrop, " Software Agents Prepare to Sift the Riches of Cyberspace," Science, 12 Aug 1994, pp 882-3; "The Keys to the Future," Business Week, 13 Jun 1994, pp 55-56; Karen Wright, "The Road to the Global Village," Scientific American, Mar 1990, pp 93-94.

35. Arthur Knoth, "Disabling Technologies: A Critical Assessment," International Defense Review, Jul 94, pp 34-5.

36. James W. Rawles, "Directed Energy Weapons: Battlefield Beams," Defense Electronics, Aug 1989, pp 48-51.

37. James W. Rawles, "Directed Energy Weapons: Battlefield Beams," Defense Electronics, Aug 1989, pp 52-53; Arthur Knoth, "Disabling Technologies: A Critical Assessment," International Defense Review, Jul 94, p 37.

38. A variation on this theme is presented in John Naisbitt, Global Paradox, (NY: William Morrow, 1994); and James Burke, "Technology and the New World Order," Byte, Dec 1992, p 324.

39. As a current example, international conglomerate corporations have given significantly more freedom to local affiliates in order to deal more effectively with local conditions and the increased speed and complexity of interaction, but to increase collective wealth production, further reinforcing the system. The empowerment occurs synergistically from both centrality and freedom. Furthermore, this experience exists in varying degrees of scale--even small companies have found it necessary to reorganize into smaller functional teams. One excellent discourse on this situation and response is found in Tom Peters, Liberation Management, (London: Pan MacMillan, 1993).

40. Richard B. McKenzie [Walter B. Gerken Professor of Enterprise and Society at University of California Graduate School of Management] observes that he has come to learn much about "the limits of state powers in a progressively more complex and integrated world economy and about the value of spontaneous and productive order that can spring from people 'doing their own thing.'" In "The Technological Revolution," Vital Speeches, 15 Jul 1992, p 587.

41. Gordon R. Sullivan, War in the Information Age (Carlisle, PA: U.S. Army War College SSI, 6 June 1994), p 15.

42. Alvin & Heidi Toffler, War and Anti-War, (NY: Little, Brown, 1993), pp 18-25.

43. Edward W. Desmond, et al, "It's A Wired, Wired World," Time Special Issue: Welcome to Cyberspace, Spring 1995.

44. C.T. Mahabharat, "Indian Oil in Deal with IBM, TISL," Newsbytes, 19 Jul 1994.

45. "Overview of AT&T's global presence," EDGE, on & about AT&T, 22 Aug 1994.

46. Robert Bissio, "Integrated Information and Development Communication Networks," Development - The Journal of SID, no.3, 1993, p 29.

47. Pete Engardio, "Third World Leapfrog," Business Week, 13 June 1994, p 46.

48. Germond & Niebur, "Survey of Knowledg-Based Systems in Power Systems: Europe," Proceedings of the IEEE, May 1992, pp 737-740.

49. Christopher Anderson, "Russian Network Generates Sparks," Science, 8 Jul 1994, p 178.

50. Peter Ross Range, "Oman," National Geographic, May 1995, p 128.

51. Knight-Ridder, "The Town may be wired and global...," The Providence Sunday Journal, 30 Apr 1995, p A3:1.

52. John Arquilla, "The Strategic Implications of Information Dominance," Strategic Review, Summer 1994, p 30.

53. Russell Watson, et al, "When Words Are the Best Weapon," Newsweek, 27 Feb 1995, p 36.

54. Ibid. p 47.

55. Li Neng, "Minister Hu Calls For Modern Electronic Information Processing Industry," Beijing Review, 20-26 Feb 1995.

56. FBIS, "Trade Commission SIgns Contract Data Network," Daily Report - China, FBIS-CHI-95-065, 5 Apr 1995, p 23.

57. FBIS, "Telecommunications System Joins Internet," FBIS Daily Report - China, FBIS-CHI-95-072, 14 Apr 1995, pp 19-20.

58. James C. Bussert, "Chinese Destroyers Incorporate Western Technologies, Designs," Signal, March 1995, pp 53-5.

59. Pamela Pohling-Brown, "Checkered Chums," International Defense Review, Feb 1995, p38.

60. A similar concept ("Cyberwar Integrated Operational Plan") is proposed by Julie Ryan in CNA report, Offensive Information Warfare--A Concept Exploration, p 11.

61. SOF in particular also recognizes the "de-massified", responsive, small task-oriented team approach currently being deployed widely in American business, primarily in response to the transformed geo-social-technical order of the Information Age. [See especially Drucker, Post-Capitalist Society; Peters, Liberation Management; & Champy, Re-Engineering the Corporation.] SOF adverises unique economy of force, expanded options, unique capabilities, high flexibility, and greatly decentralized execution. Both SOF and Airpower have developed masterful ways & means for high leverage indirect approaches.

62. Drucker, Post-Capitalist Society, p 185. See also Thach & Woodman, "Organizational Change and Information Technology: Managing on the Edge of Cyberspace," Organizational Dynamics, Summer 1994, pp 30-46.

63. Owens, "The Emerging System of Systems."

64. Fitzsimonds and vanTol, "Revolutions in Military Affairs," Joint Force Quarterly, Spring 1994, pp 24-31. For additional RMA perspectives see: Cooper, Jeffrey R., Another View of the Revolution in Military Affairs, (Carlisle, PA: U.S. Army War College SSI, 15 Jul 1994); Mazarr, Michael J., The Revolution in Military Affairs: A Framework for Defense Planning, (Carlisle, PA: U.S. Army War College SSI, 10 Jun 1994); Patrick, John J., Reflections on the Revolution in Military Affairs, Unpublished paper, (Fairfax, VA: Techmatics Center for Security Strategies and Operations, Jan 1995).

65. Naisbitt, Megatrends, (NY: Warner Books, 1982), pp 39-53.

APPENDIX A: Understanding the Information Topography

Expert Systems & Applications. Expert systems can be both targets and weapons. Expert systems "automate repetitive, tedious, or overly complex processes."[1] They are special-purpose computer programs that, given a reliable, explicit knowledge base, are expert in some narrow problem area.[2] Typical uses of expert systems include: control, diagnosis, interpretation, prediction, design, simulation, repair, training, and planning. For these purposes, expert systems are being widely incorporated in large complex systems (including computational, communications, and mechanical systems). Typical expert systems are primarily automated management [i.e., function coordination] information systems (MIS) [e.g. Energy Management System (EMS), Traffic Signal Control System] or Supervisory Control and Data Acquisition (SCADA). These systems are increasingly used with great dependence in key civil and commercial systems. Currently, electric power systems and oil & chemical production & distribution are heavily invested in expert systems worldwide. Introduction is increasingly seen in water systems, transportation traffic control, and financial mechanisms auch as trading. Although some expert systems are given full control authority, some others retain a man-in-the-loop to handle final decisions on judgements presented by the expert system. Dependence and overall system integrity may not be closely related to this fact, since corrupting the expert system can have devastating effect regardless.

Telecommunications/networking architecture & applications. Large, dispersed, or diverse systems use networking to tie computers [and "organisms"] together. Networking employs a variety of telecommunications apparatus and techniques. Media of transmission are important to recognize (e.g. electronic, optical, RF) since this is one path to access a networked target. Routing and switching architecture is also key since this creates potential sets of vulnerable nodes. [But beware the "self-healing" properties of appropriately designed distributive systems which are capable of rerouting to circumvent disruption.] Furthermore, "operating a complex and large scale computer network or collection of computer networks is a complicated enterprise. As the number of devices involved in the system increases, the systems complexity grows exponentially. Detecting and repairing software, machine and communications link failures are extremely difficult."[3]

Data management & applications. This includes data monitoring, processing, organizing, relating, calculating, combining, and displaying, among other functions. Digital data is the computer language of information. Data will exist in various stages of processing, as well as comprising the program(s) and operating system (OS) instructions themselves. With respect to processing, data is often sensed automatically [sometimes by remote peripheral devices], relayed from another computer, or input by a human operator. The data will exist in various databases for access by the program(s) or OS. Databases take various forms and a knowledge of the target's database form is important if intending to subvert it, particularly if covert or deceptive measures are desired to endure without operator alertment to data corruption. Programs, OSs, and databases usually reside in non-volatile, long term memory. In-process data is that data which is replicated and manipulated for computation (processing) and usually resides in volatile, short term memory. Output data is generally sent to a peripheral device designed specifically for human recognition and utility, or is sent along to another computer. Because of the long term nature of programs, OSs, and databases, all are potentially good value targets. OSs are often widely understood, since they are usually widely available commercially. Corrupting them could disrupt or deny information use, but deception is unlikely since inoperability will likely be apparent to the user. Programs will be useful targets if, as is common, they conduct repetitive-type functions/computations--thus providing a degree of predictability in targeting and a reasonable expectation of attack outcome. Program access and understanding may be more difficult if it is locally designed and held. Databases and stored data files may be the target gold mine, but require significant reconnaissance to understand what they represent, how they are organized, and what they are used for, and therfore may also require a knowledge of the program(s) they relate to.

Limited function micro-computers or microchips. These narrowly functional subsystems, possibly even with very narrowly defined expert systems in residence, often exist to conduct only a few specific tasks--Consider the microchips in most modern automobiles and the limited set of tasks they accomplish, like regulating carburation, ignition, and centrally managing a few key engine performance parameters. Similar micro-computers are often employed at remote grid nodes, where flow of anything from oil to information must be sensed and routed. These micro-computers, although often operating

independently, also usually feed sensed data back to a central server computer for overall grid or network management.

APPENDIX B: Information Warfare Arsenal

Definitions are quoted or paraphrased primarily from Julie Ryan, Offensive Information Warfare--A Concept Exploration, CIM 361, (Alexandria, VA: Center for Naval Analyses, Jul 1994). Wushou Chou,ed., Computer Communications, Volume I: Principles, (NJ: Prentice Hall, 1983) pp 370-373, provided definitions of masquerading and active wiretapping. Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway, (NY: Thunder's Mouth Press, 1994) also provides interesting twists on the subject.

Active wiretapping. Involves attaching an unauthorized device , such as a computer terminal, to a communications circuit for the puprose of accessing data for collection, surveillance, modification or selective disruption.

Covert pipe. This is a communications channel that is usually hidden in a information handling or telecommunications system that is unexpected by the user, but exists usually by exploiting a design flaw. It may allow information to be transferred in unintended ways, including providing access for malicious software or for covertly retrieving data or siphoning information flow.

Data manipulation. Various ways to access stored, in-process or flowing data provide a means to alter that data. Altered or manipulated data can be used to great effect in deception, degradation, or information accentuation/clarification, among others.

Electromagnetic pulse weapons. EMP is a natural by-product of nuclear explosions, but may be deliberately produced by non-nuclear devices, including the use of conventional explosives to provide power generation. EMP weapons may be large long-term generators, or one-time use bombs. The electromagnetic nature of information systems make them susceptible to EM disruption or damage.

Flaws. Software errors, intentional or not, that allow access past designed protection measures. Flaws may be introduced in the software or information development cycle,

could be designed and emplaced by a local covert agent, or might be inserted by malicious software.

High Power Microwaves. HPM are a type of radio-frequency (RF) energy transmitted at intense power levels. HPM can effect the electromagnetic composition of an information system in ways similar to EMP. Advanced research is examining ways to specify HPM wave characteristics tailored to specific info targets.

Intelligent agent. Knowledge-based expert systems that may puposefully navigate through an information system, patrolling it, searching for specific data or program functions, then retrieving, modifying or otherwise subverting information. Some intelligent agents may have the capability to "learn" and adapt to unfamiliar information systems or changes in the target system or operating environment.

Logic bomb. A piece of computer code buried within a system, that executes when a specific system state is realized. For example, it could be buried within a program that checks for the presence of a piece of data (like a user's name or password) and is set to "explode" (deliver its malicious effects) when the specified logic state is recognized (the user's password is entered).

Logic torpedo. A variation on the virus, more closely related to the intelligent agent. The logic torpedo "homes" on a specific information subsystem and/or a specific piece of information, then delivers viral-like effects.

Masquerading. Involves attempts to gain access to an information system by posing as an authorized user.

TEMPEST devices. TEMPEST is the study and control of unintentional electronic signals emitted from information systems. TEMPEST devices can be designed to sense and exploit this electronic leakage. Examples of include exploiting info system clock synchronization for other adversary systems, or using the known clock timing to synchronize an IW response.

Time bomb. Similar to the logic bomb, but executes at a specific time rather than logic state.

Time weapon. These weapons aim to disrupt the computer's clock to disrupt or alter synchronization, affecting internal or external data communication.

Trap door. A hidden software or hardware mechanism that permits system protection to be circumvented, normally activated in some nonapparent manner. Trap doors are commonly intentionally designed into software to permit correction of unanticipated bugs. These trap doors may be subject to compromise; others may be maliciously created by a covert agent.

Trojan horse. A computer program with an apparently or actually useful function, but with additional malicious functions. For example a database management program may have a Trojan horse that deletes or alters all sets of data related to a particular information characteristic.

Viruses. Viruses are programs that stealthily infect other programs, self-replicating and spreading within a computer or network, with potential to corrupt all resident data. Typically small, they are difficult to detect. In fact, some of the more recent versions have active anti-detection protection measures. Viruses may be encrypted, compressed, or polymorphic to rduce probability of detection, or to make countermeasures more difficult.

Worms. Similar to viruses, worms are self-replicating, but not parasitic (i.e., they don't attach to other programs). As demonstrated dramatically by the "Internet Worm" of 1988, they can deny legitimate users access to systems by overwhelming those systems with their progeny. Worms attack availability, whereas other weapons may attack the integrity of data or compromise confidentiality.

NOTES TO APPENDICES

1. Louis E. Frenzel, Jr., Crash Course in Artificial Intelligence and Expert Systems, (Indianapolis, IN: Howard W. Sams, 1987), p 73.

2. Donald A. Waterman, A Guide to Expert Systems, (Reading, MA: Addison-Wesley, 1986), p 4.

3. Vinton G. Cerf, "Networks," Scientific American Special Issue: The Computer in the 21st Century, 1995, pp 52-3.

BIBLIOGRAPHY

Ackerman, Robert K. "Direct Satellite Telephony Offers Terrestrial Linkage." Signal. Apr 1995. pp 26-29.

Alberts, David S. The Future of Command and Control with Dominant Battlefield Awareness. Unpublished paper. Washington, DC: National Defense University, 1995.

Anderson, Christopher. "Russian Network Generates Sparks." Science. 8 Jul 94. p 178.

Anderson, Jim, et al. "Getting the Most From Advanced Process Control." Chemical Engineering. Mar 1994.

Arnold, H.D., et al. "Targeting Financial Systems as Centers of Gravity: 'Low Intensity' to 'No Intensity' Conflict." Defense Analysis. Aug 1994. pp 181-208.

Arquilla, John. "The Strategic Implications of Information Dominance." Strategic Review. Summer 1994. pp 24-30.

Arquilla, J. & Ronfeldt, D. "Cyberwar is Coming!" Comparative Strategy. v.12, no.2, 1993. pp 141-165.

Balu, N.J., et al. "Review of Expert Systems in Bulk Power System Planning and Operation." Proceedings of the IEEE. May 1992. pp 727-731.

Beyerchen, Alan. "Clausewitz, Nonlinearity, and the Unpredictability of War." International Security. Winter 1992/93. pp 59-90.

Bissio, Roberto. "Integrated Information and Development Communication Networks." Development - the Journal of SID. v.3, 1993. pp 27-30.

Bodnar, John W. "The Military Technical Revolution: From Hardware to Information." Naval War College Review. Summer 1993. pp 7-21.

Braunberg, Andrew C. "Space-Based Telephone Service Nears Reality." Signal. Apr 1995. pp 31-33.

Brinkman, David, ed. Jane's Avionics - Thirteenth Edition. Coulsdon, Surrey, UK: Jane's Information Group, 1994.

Burke, James. "Technology and the New World Order." Byte. Dec 1992. p 324.

Busey, James B. "Information Superiority Dashes Thorny Power Projection Issues." Signal. Nov 1994. p 13.

Bussert, James C. "Chinese Destroyers Incorporate Western Technologies, Designs." Signal. Mar 1995. pp 53-55.

Campen, Alan D. "Information Warfare is Rife with Promise, Peril." Signal. Nov 1993. pp 19-20.

Cerf, Vinton G. "Networks." Scientific American Special Issue. 1995. pp 44-53.

Chen-Ching Liu. "Knowledge-Based Systems in Electric Power Systems." Proceedings of the IEEE. May 1992. pp 659-662.

Clancy, Tom. Armored Cav. NY: Berkley Books, 1994.

Collins, John M. "Where Are Special Operations Forces?" Joint Force Quarterly. Autumn 1993. pp 7-16.

Collins, Catlin, & Ilges. "Expert Systems Assist Operators." American Water Works Association Journal. Dec 1994. p 18.

"The Computer in the 21st Century." Scientific American Special Issue. 1995. pp 4-9.

"Controlling oil flow on-shore." Process Engineering. 22 March 1992.

Cooper, Jeffrey R. Another View of the Revolution in Military Affairs. Carlisle, PA: U.S. Army War College SSI, 15 Jul 1994.

Corbin, Lisa. "Open Systems: The Key to Computer Interoperability." Government Executive. Jun 1992. pp 55-6.

Cullen & Foss, eds. Jane's AFV Retrofit Systems, Seventh Edition. Coulsdon, Surrey, UK: Jane's Information Group, 1994.

"Dealing with Worms and Viruses." in Madron, Thomas W. Network Security in the '90s - Issues and Solutions for Managers. NY: John Wiley & Sons, 1992.

DeLanda, Manuel. War in the Age of Intelligent Machines. NY: Zone Books, 1991.

Dertouzos, Michael L. "Communications, Computers and Networks." Scientific American Special Issue. 1995. pp 22-29.

Emmett, Peter C. "Software Warfare - The Militarization of Logic." Joint Force Quarterly. Summer 1994. pp 84-90.

Emmett, Peter C. "Software Warfare: The Emerging Future." The RUSI Journal. Dec 1992. pp 56-60.

Engardio, Pete. "Third World Leapfrog." Business Week. 13 Jun 1994. pp 46-7.

Esposito, Joseph J. "Future of Knowledge." Vital Speeches. 15 Aug 1993. pp666-668.

Finley, Michael. "Making It Just in Time." Beyond Computing. Mar 1995. pp 49-50.

Fitzsimonds, James R. & Van Tol, Jan M. "Revolutions in Military Affairs." Joint Force Quarterly. Spring 1994. pp 24-31.

Flanagan, P. "Future Industry Directions: The 10 Hottest Technologies in Telecom." Telecommunications. May 1994. pp 31-38+.

Foreign Broadcast Information Service. "China to Set Up 1st High Tech Conglomerate." Daily Report: China. FBIS-CHI-95-068. 10 Apr 95. p 32.

Foreign Broadcast Information Service. "Telecommunications System Joins Internet." Daily Report: China. FBIS-CHI-95-072. 14 Apr 95. pp 19-20.

Foreign Broadcast Information Service. "Trade Commission Signs Contract for Data Network." Daily Report: China. FBIS-CHI-95-065. 5 Apr 95. p 23.

Foreign Broadcast Information Service. "UN Official on Telecommunications in Tumen Valley." Daily Report: China. FBIS-CHI-95-068. 10 Apr 95. pp 32-3.

Frankel, Charles. "Change and the Future." in Walker, Charles R. Modern Technology and Civilization. NY: McGraw-Hill, 1962.

Franks, Frederick M., Jr. "Winning the Information War." Vital Speeches. 15 May 1994. pp 453-458.

Frenzel, Louis E., Jr. Crash Course in Artificial Intelligence and Expert Systems. Indianapolis, IN: Howard W. Sams, 1987.

G.T. Global Financial Services. Investing in the Information Age: G.T. Global Telecommunications Fund Investment Information. San Francisco, CA: 1994.

Germond & Niebur. "Survey of Knowledge-Based Systems in Power Systems: Europe." Proceedings of the IEEE. May 1992. pp 732-744.

Gilder, George. "Into the Fibersphere." Forbes ASAP. 7 Dec 1992. pp 111-125.

Gingrich, Newt. Unpublished text of speech on "Information Warfare" to AFCEA Conference. Arlington, VA: 8 Feb 1995.

Gleick, Peter H. "Water ans Conflict: Fresh Water Resources and International Security." International Security. Summer 1993. pp 79-112.

Gore, Al. "Infrastructure for the Global Village." Scientific American Special Issue. 1995. pp 156-9.

Gore, Al. "The National Information Infrastructure." Vital Speeches. 1 Feb 1994. pp 229-233.

Hammer, M. & Champy, J. Reengineering the Corporation. NY: Harper Business, 1993.

Handel, Michael I. Sun Tzu and Clausewitz: The Art of War and On War Compared. Carlisle, PA: U.S. Army War College SSI, 1991.

Handel, Michael I. "Clausewitz in the Age of Technology." in Handel, ed. Clausewitz and Modern Strategy. London: Frank Cass, 1986.

Hardy, Stephen M. "Finding A Place On Board - EW Payloads for UAVs." Journal of Electronic Defense. Feb 1992. pp 28-34+.

Hewish, Mark. "Fishing in the Data Stream: Netting Information is the Trick." International Defense Review. Jul 1994. pp 51-6.

Hughes & Dornheim. "Accidents Direct Focus on Cockpit Automation." Aviation Week & Space Technology. 30 Jan 1995. pp 52-4.

"Information Dominance Edges Toward New Conflict Frontier." Signal. Aug 1994. pp 37-40.

Jackson, James O. "It's a Wired, Wired World." Time Special Issue: Welcome to Cyberspace. Spring 1995. pp 80-82.

Jeremiah, David E. "What's Ahead for the Armed Forces?" Joint Force Quarterly. Summer 1993. pp 25-35.

Kane, Les A. "Understanding Modern Control Jargon." Hydrocarbon Processing. Oct 1994.

Kelly, Brian J. "Command and Control Basics Enhance Explosion of Information Technology." Signal. Mar 1995. pp 15-16.

"The Keys to the Future." Business Week. 13 Jun 1994. pp 52-9.

Kirschen & Wollenberg. "Intelligent Alarm Processing in Power Systems." Proceedings of the IEEE. May 1992. pp 663-672.

Kitfield, James. "Trading Bullets for Bytes." Government Executive. June 1994. pp 19-22.

Knight-Ridder. "The town may be wired and global, but its preference is local." The Providence Sunday Journal. 30 Apr 1995. p A3:1-6.

Knoth, Arthur. "Disabling Technologies: A Critical Assessment." International Defense Review. Jul 1994. pp 32-9.

Lewonoski, Mark C. Information War. Unpublished paper. Naxwell AFB, AL: Air War College, Apr 1991.

Libicki, Martin C. & Hazlett, James A. "Do We Need An Information Corps?" Joint Force Quarterly. Autumn 1993. pp 88-97.

Liddell Hart, B.H. Strategy - The Indirect Approach. NY: Frederick A. Praeger, 1949.

Lind, William S., et al. "The Changing Face of Warfare: Into the Fourth Generation." Military Review. Oct 1989. pp 2-11.

Li Ning. "Minister Hu Calls For Modern Electronic Information Processing Industry." Beijing Review. 20-26 Feb 1995. pp 12-17.

Littlewood & Strigini. "The Risks of Software." Scientific American Special Issue. 1995. pp 180-5.

Lovicsek, Kelman, & Stewart. "Integrated Traffic Control Center for Metro Toronto." ITE Journal. Dec 1992. pp 35-39.

Lum, Z. "C2W Payloads for UAVs." Journal of Electronic Defense. Jan 1995. pp 36-7.

Luoma, William M. Netwar: The Other Side of Information Warfare. Unpublished paper. Newport, RI: U.S. Naval War College, 8 Feb 1994.

Luoma, William M. The Computer Virus: Weapon of Mass Destruction? Unpublished paper. Newport, RI: U.S. Naval War College, 14 Feb 1994.

Macioti, Manfredo. "Innovation and diffusion of technology: an example of the printing press." Impact. v.39, no.2, 1989. pp 143-150.

Mahabarat, C.T. "Indian Oil in deal with IBM, TISL." Newsbytes. 19 Jul 94.

Mallory, Jim. "Control Data gets Russian automation contract." Newsbytes. 15 Jun 1994.

Matsumoto, K., et al. "Knowledge-Based Systems as Operational Aids in Power System Restoration." Proceedings of the IEEE. May 1992. pp 689-697.

Mayo, John S. "Communications After 2000 AD." Vital Speeches. 15 Jul 1992. pp 599-603.

Mazarr, Michael J. The Revolution in Military Affairs: A Framework for Defense Planning. Carlisle, PA: U.S. Army War College SSI, 10 Jun 1994.

McKenzie, Richard B. "The Technological Revolution." Vital Speeches. 15 Jul 1992. pp 587-595.

Mellor, Richard. "The changing face of SCADA systems." Process Engineering. Jan 1993.

Mowlana, Hamid. "Information Hunger and Knowledge Affluence: How to Bridge the Gap?" Development - The Journal of SID. v.3, 1993. pp 23-6.

Mumford, L. "Two Views on Technology and Man." in Thrall & Starr, eds. Technology, Power, and Social Change. Lexington, MA: Lexington Books, 1972.

Naisbitt, John. Global Paradox. NY: William Morrow, 1994.

Naisbitt, John. Megatrends: Ten New Directions Transforming Our Lives. NY: Warner Books, 1982.

Nordwall, Bruce D. "Standards Main Hurdles to New ATC Technologies." Aviation Week & Space Technology. 16 May 1994. pp 46-7.

Nordwall, Bruce D. "Avionics Market To Improve In '96." Aviation Week & Space Technology. 13 Mar 1995. pp 81-3.

"Overview of AT&T's global presence: August 1994." EDGE, on & about AT&T. 22 Aug 1994.

Owens, William A. "The Emerging System of Systems." Naval Institute Proceedings. May 1995. pp 35-9.

Owens, William A. High Seas: The Naval Passage to an Uncharted World. Annapolis, MD: Naval Institute Press, 1995.

Owens, William A. "JROC: Harnessing the Revolution in Military Affairs." Joint Force Quarterly. Summer 1994. pp 55-7.

Patrick, John J. Reflections on the Revolution in Military Affairs. Unpublished paper. Fairfax, VA: Techmatics Center for Security Strategies and Operations, Jan 1995.

Payton, Gary D. "The Art of Intelligence, By the General." Airpower Journal. Winter 1993. pp 16-25.

Peters, Tom. Liberation Management - Necessary Disorganization for the Nanosecond Nineties. London: Pan Macmillan, 1993.

Plafker, Ted. "China to Triple Internet Links With Commercial Hookups." Science. 13 Jan 1995. p 168.

Pohling-Brown, Pamela. "Checkered Chums: Regional geopolitics and the potentially lucrative Chinese marketplace have encouraged some unusual bedfellows." International Defense Review. Feb 1995. p 38.

Range, Peter R. "Oman." National Geographic. May 1995. pp 112-138.

Rawles, James W. "Directed Energy Weapons: Battlefield Beams." Defense Electronics. Aug 1989. pp 47-54.

Rawles, James W. "High Technology Terrorism." Defense Electronics. Jan 1990. pp 74-76.

Roberts, Bert C., Jr. "Information Highways Delivering and Shaping." Vital Speeches. 1 Feb 1994. pp 233-6.

Rumpel & Krost. "Natural Language Interface and Database Issues in Applying Expert Systems to Power Systems." Proceedings of the IEEE. May 1992. pp 758-764.

Ryan, Donald E., Jr. "Implications of Information-Based Warfare." Joint Force Quarterly. Winter 1994-95. pp 114-116.

Ryan, Julie. Information Support to Military Operations in the Year 2000 and Beyond: Security Implications. CIM 324. Alexandria, VA: Center for Naval Analyses, Nov 1993.

Ryan, Julie. Offensive Information Warfare - A Concept Exploration. CIM 361. Alexandria, VA: Center for Naval Analyses, Jul 1994.

Sanders, Ralph. "Integrating Technology, Military Strategy, and Operational Concepts." in Margiotta & Sanders, eds. Technology, Strategy and National Security. Washington, DC: National Defense University Press, 1985.

Sandoval, Victor. "Computers, telematics, and road freight management." Impact. v.41, no.2, 1991. pp 127-136.

Scheer, Christopher. "Third Wavers & Tekkie Cults: The Pursuit of Techno-Happiness." The Nation. 8 May 1995. pp 632-4.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. NY: Thunder Mouth Press, 1994.

Scott, William B. "Information Warfare Demands New Approach." Aviation Week & Space Technology. 13 Mar 1995. pp 85-8.

Seaman, Barrett. "The Future is Already Here." Time Special Issue: Welcome to Cyberspace. Spring 1995. pp 30-33.

"Security in Computer Communications Systems." in Chou, W., ed. Computer Communications. Volume 1: Principles. Englewood Cliffs, NJ: Prentice-Hall, 1983.

Seifried, Carl. "Merging GIS and SCADA." American City & County. Oct 1994.

Sekine, Y., et al. "Fault Diagnosis of Power Systems." Proceedings of the IEEE. May 1992. pp 673-683.

Smith, Carrie R. "Emerging Markets Ride The Electronic Wave." Wall Street & Technology. Apr 1994. p 38-43.

Smith, Raymond W. "The Global, Interactive, Human Network." Vital Speeches. 1 Sept 1993. pp 691-695.

Soon, D.M. "Remote Access: Major Developments in 1995." Telecommunications. Jan 1995. pp 57-8.

Spear, Mike. "SCADA takes control of cross-country oil flows." Process Engineering. Jan 1992.

Steele, Robert D. "Cyber War." Marine Corps Gazette. Oct 1994. pp 79-80.

Stewart, John F., Jr. "Command and Control Warfare and Intelligence on the Future Battlefield." Army Research and Acquisition Bulletin. Nov-Dec 1994. pp 14-15.

Stix & Wallich. "A Digital Fix for the Third World?" Scientific American Special Issue. 1995. p 43.

Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. NY: Doubleday, 1989.

Sullivan, Gordon R. & Dubik, James M. War in the Information Age. Carlisle, PA: U.S. Army War College SSI, 6 Jun 1994.

Swett, Charles. "Review Essay: War and Anti-War." Special Warfare. Jan 1995. pp 26-31.

Szafranski, Richard. "Neocortical Warfare? The Acme of Skill." Military Review. Nov 1994. pp 41-55.

Talukdar, S., et al. "Multiagent Organizations for Real-Time Operations." Proceedings of the IEEE. May 1992. pp 765-778.

Thach & Woodman. "Organizational Change and Information Technology: Managing on the Edge of Cyberspace." Organizational Dynamics. Summer 1994. pp 30-46.

"Threats to Computer/Communication Systems." in Bartee, Thomas C., ed. Data Communications, Networks, and Systems. Indianapolis, IN: Howard W. Sams, 1985.

Toffler, Alvin. The Third Wave. NY: Wm Morrow, 1980.

Toffler, Alvin & Heidi. War and Anti-War. Boston: Little, Brown, 1993.

U.S. Air Force Dept. Basic Aerospace Doctrine of the United States Air Force. AFM 1-1, Vol. 1. Washington, DC: Mar 1992.

U.S. Army Dept. Doctrine for Special Operations Forces. FM 31-20. Washington, DC: 20 Apr 1990.

U.S. Army Training and Doctrine Command. Information Operations. Draft FM 100-6. Ft.Monroe, VA: 22 Jul 94.

U.S. Department of Defense (OASD Special Operations and Low-Intensity Conflict; and CINC Special Operations Command). United States Special Operations Forces Posture Statement. Washington, DC: 1994.

U.S. Joint Chiefs of Staff (Chairman). Command and Control Warfare. Memorandum of Policy No. 30, 1st Revision (CJCS MOP 30). Washington, DC: 8 Mar 1993.

U.S. Joint Chiefs of Staff. Doctrine for Intelligence Support to Joint Operations. Joint Pub 2-0. Washington, DC: 12 Oct 1993.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington, DC: 9 Sept 1993.

U.S. Joint Chiefs of Staff. Doctrine for Joint Special Operations. Joint Pub 3-05. Washington, DC: 28 Oct 1992.

U.S. Joint Chiefs of Staff (J-6). "Committed, Focused, and Needed" C4I for the Warrior. Washington, DC: 12 June 1993.

U.S. Navy Dept. Implementing Instruction for Information Warfare/ Command and Control Warfare (IW/C2W). OPNAVINST 3430.26. Washington, DC: 18 Jan 1995.

U.S. Navy Dept. Naval Command and Control. Draft NDP 6. Norfolk, VA: Naval Doctrine Command, Dec 1994.

Ubios, Jeff. "The biggest, meanest market: China wants digital media, but on its own terms." Digital Media. 13 Sep 1994.

Valovic, Tom. "Quality of Information--Part II." Telecommunications. Jan 1995. p 8.

Van Dusen Wishard, Wm. "A New Frame of Reference." Vital Speeches. 15 Dec 1994. pp 153-8.

Waldrop, M. Mitchell. "The Seeds of the Internet Boom." Science. 12 Aug 1994. pp 880-881.

Waldrop, M. Mitchell. "Software Agents Prepare to Sift the Riches of Cyberspace." Science. 12 Aug 1994. pp 882-3.

Walker, Charles R. Technology, Industry, and Man - The Age of Acceleration. NY: McGraw-Hill, 1968.

Wallich, Paul. "Wire Pirates." Scientific American Special Issue. 1995. pp 186-194.

Waga, Phil. "PC Power Surge." The Reporter Dispatch. Yorktown Heights, NY: Gannett Suburban Newspapers, 10 May 1995. pp 1:2-4 - 2:1-5.

Warden, John A., III. "Employing Air Power in the Twenty-first Century." in Shultz & Pfaltzgraff, eds. The Future of Air Power in the Aftermath of the Gulf War. Maxwell AFB, AL: July 1992.

Waterman, Donald A. A Guide to Expert Systems. Reading, MA: Addison-Wesley, 1986.

Watson, Russell, et al. "When Words Are the Best Weapon." Newsweek. 27 Feb 1995. pp 36-40.

"Welcome to Cyberspace." Time Special Issue: Welcome to Cyberspace. Spring 1995. pp 4-11.

Wright, Karen. "The Road to the Global Village." Scientific American. Mar 1990. pp 84-94.

Wurman, Richard S. Information Anxiety. NY: Doubleday, 1989.