AIR WAR COLLEGE

AIR UNIVERSITY

THE

END OF SECRECY?

MILITARY COMPETITIVENESS IN THE AGE OF TRANSPARENCY

By

Beth M. Kaspar, LtCol USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Dr. Grant Hammond and Mr. Ted Hailes

Maxwell Air Force Base, Alabama

April 2000

Air War College
Maxwell AFB, Al 36112

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Figures

Page

Preface

This study focuses on military competitiveness in the age of transparency. My thesis asserts that the US military must consciously prepare itself to fight in an information transparent world created by globalization. The worldwide explosion in the quantity and quality of information and products available to the general public user, the ready accessibility to the information, and the affordability in acquiring any desired data or product is creating a transparent world at an alarming rate. In the future, anyone can affordably keep tabs on the actions of everyone else. Hence, the US military must consciously begin to investigate ways to maintain its military advantage in this rapidly evolving transparent world. It must minimize the impact transparency has on how we will fight wars and conduct contingency actions. We must not be caught by surprise. If I convince you that we need to begin now addressing the downstream impacts, then this paper is a success. Maintaining US military competitiveness will require a multifaceted solution - of which I have only scratched the surface. Well thought through solutions are left for Scientific Advisory Boards, War Colleges, and others for action.

My sincere thanks to Dr. Grant Hammond and Col. (Ret) Theodore Hailes of the Air War College's Center for Strategy and Technology (CSAT) for giving me the opportunity to conduct this research. Thanks also to Mr. Ted Kluz, Dr. Joseph Aein, Col. (Ret) Dr Randy Gressang, and Col. (Ret) Joe Bianco for taking the time to challenge my thesis, debate the issue, and provide invaluable advice regarding this study.

Abstract

Information and communications technologies are having a profound impact, both domestically and globally, on how future war is waged. These technologies are providing affordable, worldwide, near real-time, 24-hour, CNN-like news coverage, worldwide Internet access, and more importantly, access to commercial space systems, including remote sensing, communications and navigation. Unfortunately, this explosion in worldwide information and communication systems creates vulnerabilities for US national security. One such vulnerability is information transparency. Transparency is the result of the worldwide explosion in quantity and quality of information available to the general user, the accessibility to the information, and the affordability in acquiring any data product desired. The resultant electronic information symmetry makes the world transparent, where any one can keep tabs on the actions of everyone else.

This study investigates how the US can retain its military advantage in the coming age of transparency. The inevitable economic pressure of the "web," or more generally information e-commerce, is advancing the rate of global transparency. Relying only on the National Command Authority to continue with its approach of controlling information release to the public is doomed. Transparency can seriously degrade several principles of war, most significantly mass, maneuver, and surprise. For example, it will provide an adversary near-real time, accurate battle-space visibility of US military posture at both the strategic and theater levels. As such, an adversary could preemptively

deny forward basing by destroying air bases or sea ports, use his own long range precision strike weapons against pre-selected US targets, and selectively deny US-developed space based navigation to counter surprise attacks. In essence, transparency affects military capability - for both sides - in temporal and spatial dimensions.

US military planners must accept that information transparency is inevitable and then proceed to minimize its affects on our military capability. Deliberate innovation in doctrine, advanced weapon systems, and organizational structures must be initiated to mitigate the speed and clarity, or celerity, that information transparency provides. Only by being prepared, can the US maintain its competitive military edge.

Chapter 1

Introduction

Rapidly emerging information and communications technologies are going to profoundly impact how future war will be waged. The increasing availability of high-quality commercial satellite based communications, navigation, and surveillance information, ready access to the Internet or other worldwide computer networks, and 24 hour worldwide media coverage to virtually anyone who wants it may be a great equalizer in future conflicts. No longer can nation states control information release to the general public and the rest of the world. Because of the irrevocable, accelerating progress of information sciences and economic globalization, information "e-commerce" is advancing at exponential rates. In the future, virtually anyone will be able to play. Unfortunately, denying or delaying access to "bad actors" may be difficult or impossible technically, politically, and legally.[1] Consequently, several military advocates have argued that space weapons could selectively destroy critical elements of this transparency in time of need to ensure US information dominance.

The US National Command Authority (NCA) favors a more deliberate approach to unleashing offensive weapons in space. As the world's last remaining superpower, employing space weapons outside of some dire, overwhelming circumstance will be unjustifiable to the international community. Furthermore, until a "dire circumstance" is thrust upon the US, it is not reasonable to expect the NCA to prepare and train for the employment of space weapons. Some experts even question whether such weapons would be effective. New satellite systems, they argue, are less vulnerable to disruption because software automatically reroutes traffic when a satellite goes down.[2] Thus, the most likely environment the US military will face in the near future is "information transparency" where anyone can keep tabs on the actions of everyone else.

This study investigates how the US military can remain competitive in an age of transparency. Chapter 2 looks at how the world is becoming more information transparent. Transparency is the result of the explosion in affordable, robust commercial satellite services, rapid evolution in dual use technology, and expanding demand for continuous worldwide news coverage.[3] This technology diffusion is moving our society from an environment wherein nation-states have controlled the dispersion of advanced technology to a more information open, anarchic global society. Chapter 3 addresses the impact this emerging transparency has on the US ways of warfare. Transparency degrades several US principles of war, principally mass, maneuver, and surprise. Examples are included on how a potential adversary could exploit transparency to deny to the US power projection. Specifically, an adversary may use commercially acquired near-real time images for accurate battle-space visibility, employ market accessible components to develop long-range accurate precision strike weapons, and then combine them to deny the airbases or seaports needed for US force projection or hold at serious risk forward deployed US military assets. . The chapter concludes with a look at how transparency impacts US preferences for fighting as part of a coalition and using technology as a force multiplier. Chapter 4 explores possible steps the US military can take to mitigate the affects of transparency. Deliberate innovation in doctrine, more robust advanced weapon system procurement, and organizational adaptation must be initiated to mitigate the celerity, or speed and clarity, that information transparency provides to a potential adversary. By conducting realistic "red/blue" force war games, the Armed Forces can develop alternative strategies to nullify the diffusion of technology and its real-time data consequences. By understanding the emerging vulnerabilities, we can seek to counteract them. These vulnerabilities include evaporating geographic sanctuary, growing global data parity, and regional power offensive attacks using selective equal technologies.

Information transparency is economically plausible and an increasing reality. Consequently, the US military must begin preparing itself to maintain a superior stance in the age of transparency -- either through negating its affects or developing new areas of strength. The ability of US doctrine, organization, and procurement system to counter this increasing degree of global transparency, where anyone can know anything about everyone else, is vital.

Notes

[1] Buchan, Glenn, "Information War and the Air Force: Wave of the Future? Current Fad?", Issue Paper, RAND, March 1996.

[2] Crock, Stan, "Space: The Final Battleground?", *Business Week*, 15 June 98, Issue 3582, p. 122.

[3] In the past, many of the DOD science and technology achievements, designed to maintain a technologically superior military force, have progressed to the civilian economy and formed the basis of technological advancement in industry. Today, there is much movement of technology in the other direction, from the commercial world to defense.

Chapter 2

Shifting Secrecy

"Global dominance will be achieved by those that most clearly understand the role of information and the power of knowledge that flows from it."

Adm. David E. Jeremiah
Former Vice Chairman, Joint Chiefs of Staff

In April 1986, Moscow remained tightlipped about a rumored leak of nuclear byproducts at its Chernobyl nuclear facility; but a US government "Keyhole" satellite captured an unobstructed view of the damaged power plant. Only twenty-four hours after the Pentagon analysts first saw the wreckage, ABC News broadcast the same view obtained from a commercial satellite. The pictures were blurry, but the underlying message was clear.[4] The age of total government monopoly on high-tech surveillance was over.

Increasingly, technologies and their information products that were once the exclusive preserve of the US and USSR governments are available commercially for purchase. Spurred by global competition, advances in commercial technology, and a loosening of Cold War governmental restrictions, information related technologies are on the open market at affordable prices. High performance computers, satellite imagery, and cryptographic technology are just a few of the traditionally closely held technologies now available globally to individuals or commercial entities. Furthermore, countries can exploit the easing access to dual use technologies to develop new systems or modify existing systems, such as high performance computers and optical surveillance satellite technology.[5] Another example is a strap-down inertial navigation system for ballistic and cruise missile high-accuracy guidance using computer chips identical to those used in commercial products.[6] Similarly, countries like Iraq can use civilian telephone system compliant to the standards of the International Telecommunications Union (a subsidiary of the UN), including fiber optic cable, to create a strategic command and control system.

In the following sections, areas contributing to increasing international transparency will be reviewed individually. These areas include global access to commercial satellite products, high speed Internet access, worldwide, twenty-four hour media coverage, and dual use technologies. It is important to gain an understanding of the nature of transparency before an assessment can be made on the impact to future war.

Commercial Space

Once the exclusive purview of superpower governments, space technology is rapidly becoming commercial. In fact, commercial firms are investing in space technologies at an unprecedented rate. This year market revenues are expected to top $2 billion, increasing more than six-fold in five years.[7] Several factors contribute to this dramatic growth. Within the last five years we have seen a rapid shift in communications traffic due to the convergence of computer and communications technology. This rapid evolution of information technologies, such as the extraordinary advances in digital signal processing and complex modulation schemes as well as voice and video data compression, allow for increased effective bandwidth for commercial satellite communications. Second are changes in international space policy, which are driven by deregulating telecommunications services and new frequency spectrum allocations for commercial satellite communications service. Third, is the growing dual use aspect of many information technology systems, like the Global Positioning System (GPS). GPS is finding rapid acceptance around the world, with Japan being the second largest manufacturer of GPS systems after the US.[8] Lastly are the fundamental changes in the processes and cost of satellite manufacturing and expanding global demand for satellite services driven by the information revolution.[9] In general, business entrepreneurs are finding commercial satellites and their products to be affordable, reliable, and profitable.

Space-Based Telecommunications. Such an area undergoing significant commercial transformation is satellite-based telecommunications. As governments, businesses, and individuals around the world want more information faster, they look to satellites to provide it efficiently and inexpensively. A recent Leslie Taylor Associates study predicts global Mobile Satellite Services (MSS) will build on a tremendous growth of services creating a $25 billion market by the year 2004. Subscribers are projected to increase from a current 400,000 to 24 million within five years.[10] Furthermore, according to a 1998 analysis from Booz-Allen and Hamilton, a major international consulting firm, the annual potential for US global broadband services will grow to nearly $200 billion by 2005 and space-based broadband services will capture 15% of that market.[11]

Major new satellite communications systems are being deployed in the low, medium and traditional geo-stationary earth orbits, or a combination of medium and geo-stationary orbits.[12] The "big low earth orbit (LEO)" systems are in the 1-2 GHz range and provide voice and data communications, especially mobile telephone service.[13] Proposed systems include Signal (Russian), ICO Global (a 79-nation consortium) and European-African Satellite Telecom (Marconi-Matra). (Note: the US companies

Globalstar and Iridium have filed for bankruptcy protection.) The "little LEO" systems, such as Orbcomm (US) and Starsys (US), operate below 1 GHz and provide data communications such as e-mail, two-way paging, and messaging to remote locations.[14] Broadband LEO systems provide high-speed data services such as video conferencing and high end Internet access via a Ka-band frequency.[15] Example systems include Teledesic (US), Skybridge (a joint venture by Loral (US) and Alcatel Alsthom), Celestri (European) and Wide-band European Satellite Telecommunications. In geo-stationary orbit, several new satellite systems are under development. Example systems, such as Cyberstar, Spaceway, Astrolink, and Eurosky Way, are designed to provide global, two-way broadband capability to meet the needs for voice, data, interactive multimedia, and video teleconferencing.[16] A new type of system is the hybrid low and geo-synchronous earth orbiting system. Service providers let the customer choose whether a given application is better sent to a low earth orbiting satellite – where near real-time response is desired or a higher geo-synchronous earth orbiting satellite, for applications of a longer duration. For instance, an Internet user could order a video via a low earth orbiter and have the order filled by a higher geo-synchronous orbiter.[17] While this market faces extreme competition from the cellular phone industry, it does open up possibilities to governments and militaries around the world to affordably lease space-based 50MHz transponders.

Increasingly, both industry and the US military are relying on leased commercial, primarily geo-synchronous, space communications, such as INMARSAT and PANAMSAT, to provide the long haul communications pipe between the US and forward operating locations. In Bosnia, the US military leased a commercial wide-band direct broadcast system to provide reconnaissance data, weather, intelligence on demand, and even Cable News Network to about 30 different locations at 24 megabits a second.[18] This innovative use of commercial communications satellites has fueled the military's appetite for more.

The US military already leases space on commercial communications satellites to augment its own resources. Many US Navy warships are equipped with the INMARSAT commercial communication system, allowing voice communications nearly anywhere on the globe.[19] The desire for communications connectivity is on the rise. In Operation Allied Force in Kosovo, the Allies connected 40 different locations in 15 different countries using a variety of military and civilian lines and satellites.[20] The AF is now evaluating the option of launching dedicated military space-based communications transponders aboard new broadband commercial multimedia systems such as Teledesic LLC and Hughes proposed Spaceway.[21] The Pentagon estimates that by 2008, 70% of defense communications could go through commercial satellites. Many other countries have already gone this way.[22] In short, the world is becoming utterly dependent on orbiting satellites for business, news, entertainment, international relations, navigation and everyday phone calls – as well as military command and control.

Remote Sensing. Space-based commercial remote sensing is following a path similar to commercial communications. It is becoming a very lucrative and viable business area. The growing accessibility to higher-resolution satellite imagery has been spurred by the declassification of American and Russian spy satellite archives, technological advances in higher resolution sensors for imaging satellites and geographical information systems (GIS), lower launch costs, and a growing market demand. What was once the exclusive province of the US and USSR has become available to anyone. The new generation of space-based commercial remote sensing offers any potential enemy similar higher-resolution ground intelligence, at fast revisit rates with rapid distribution for a price.

Commercial remote sensing is a dual use technology with tremendous potential – for both good and bad. Industries and governments alike recognize the valuable contribution commercial remote sensing has as an analysis tool for decision making. It supports civil applications such as weather forecasting, natural resource management, and global ecology monitoring and mapping. It supports commercial applications such as traffic management, pipeline safety, precision agricultural farming, support to media news reporting, and computer games.[23] It also supports a variety of diplomatic/military needs such as peace negotiations, treaty verification, humanitarian operations, as well as military mapping (10-meter resolution) mission planning, weapon targeting and navigation, and combat operations.[24] Or worse, as the Carnegie Endowment asserts, commercial remote sensing could encourage industrial espionage, terrorism, or more cross-border military attacks in the developing world.[25]

The improving resolution that these space-based commercial remote sensing systems are producing is concerning. Figure 1 provides a visual comparison of the various resolution levels. Ten-meter resolution is sufficient for *detecting* bridges, buildings, and even concentrations of tanks. Two-meter resolution is sufficient to *generally identify* aircraft, vehicles, roads and bridges while 1-meter resolution is sufficient to *precisely identify* types of aircraft, tanks, airport and harbor facilities, cars in railroad yards, vehicles on roads and bridges, and troop units.[26] It is also precise enough to distinguish fighter from bomber or missile launchers from trucks.

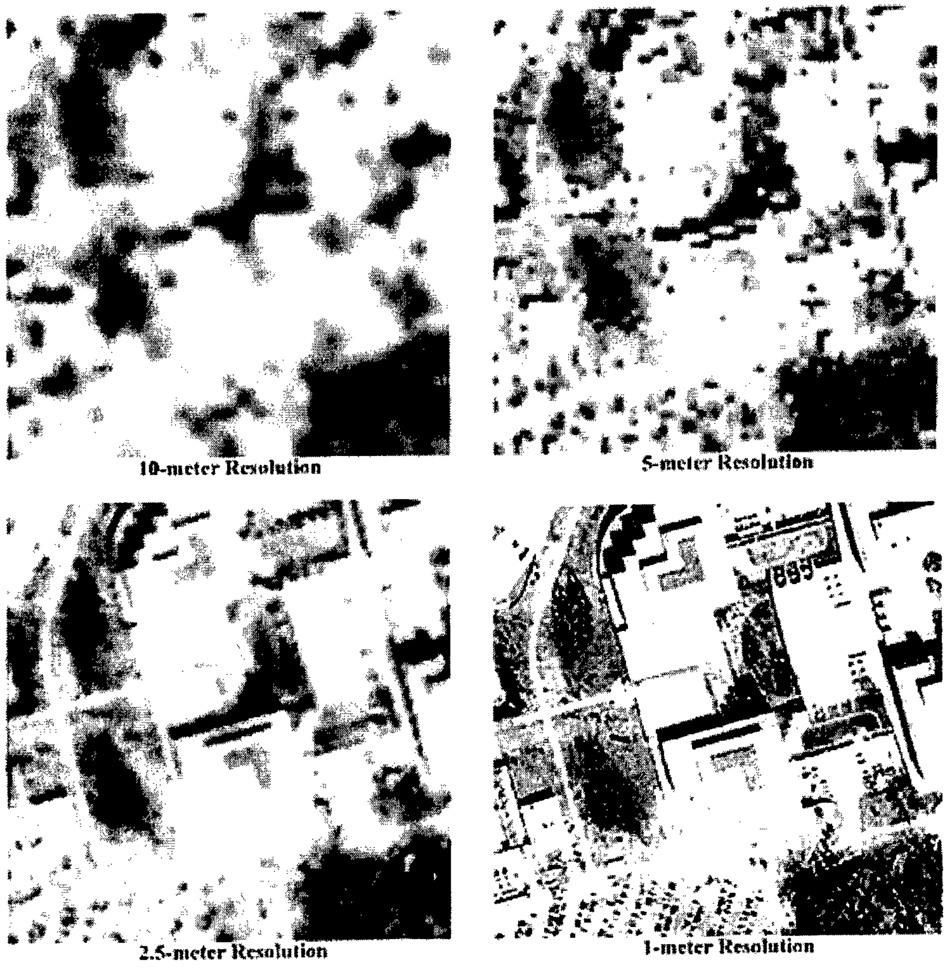


Figure 1 Samples of Commercial Image Resolution

Given the wide range in potential applications, it is not surprising that commercial remote sensing market revenue forecasts range as high as $20 billion per year.[27] Within the next decade, over 100 earth observation satellites may be launched by both private and government entities and of these over 11 companies, in five countries, are expected to launch 1-meter resolution satellites.[28] The United States, Russia, France, Israel, India, and South Korea are already developing substantial commercial remote sensing capabilities to take advantage of these applications for national economic development. This new generation of commercial satellites will not only provide imagery data of higher spatial resolution (i.e., 1-2 meters) but, just as importantly, also offer major improvements in revisit rates, geo-location accuracy, faster distribution and in some cases stereo images.

The US Space Imaging's IKONOS satellite is already providing 1 meter (or better) resolution imagery.[29] The US EarthWatch and Orbview companies plan to launch their 1-meter resolution satellites later in 2000. The Sovinformsputnik Interbranch Association in Russia has been selling 2-meter resolution images from its archives using their Sputnik era technology.[30] It is anticipated that by later this year, the Duma will authorize the sale of 1-meter resolution images.[31] The West Indian Space Ltd., a joint venture by Israeli Aircraft and California CORE Software Technology, plans to launch EROS satellites by 2002 with a resolution of 1.5 meters.[32] India plans to launch its 1-meter resolution IRS-1D satellite in 2003. South Korea rounds up the list with a projected launch in the 2003 time frame as well. Indeed, the projection is that as the number of commercial platforms in orbit soars over the next decade, high-resolution pictures from space will be routinely available, as will cloud piercing radar images and hyper-spectral scans that combine hundreds of light bands to produce intricate details about ground features.[33]

Improvements in affective resolution are possible with advanced digital signal processing. France has developed a merged data technique that simultaneously down-links the imagery taken by the same camera from one satellite via two transmission channels. It then blends, for example, two SPOT 5B 5-meter resolution images on the ground to produce a 2.5-meter resolution image.[34] It will be available for sale beginning in 2002. Undoubtedly, other commercial satellite companies will develop their own imaging sharpening techniques to create a higher resolution stereo image or unique product for sale. They may even sell the raw images to regional distributors for more innovative data manipulation.

A growing business base in commercial remote sensing is electronic image distribution and processing. Whereas remote sensing once depended on mainframe computers and highly trained dedicated experts, now advanced software, data storage, and data processing techniques allow companies to affordably process the data on desktop computers and distribute it in real-time, via CD-ROM and the Internet, with relatively ease. For example, using a desktop computer, one can easily perform GIS functions which geographically reference a large array of data, including the remotely sensed ones, manipulate and analyze it, and deliver the generated information, on time, in the customer's format. In fact, several start up companies have joined in establishing commercial remote sensing companies in distributing the commercial sensing raw and processed imagery and providing value-added analysis from these satellites. These companies are usually regional distributors for other nation's satellite company remote imagery. For example, ImStrat Corporation is the US distributor for SPOT imagery, Aerial Imagery of Raleigh NC is the distributor for the Russian 2-meter KVR-1000 satellite, and Space Imaging is the North American distributor for India's 5-meter resolution IRS family of satellites. In Europe, SPOT Imaging is the distributor for Orbital Sciences Orbview-3 and –4 satellites.[35] Furthermore, several of these distributors have been given permission to manipulate the raw data to suit customer's needs. ImStrat, for example, can sharpen a 1-meter panchromatic image with multi-spectral imagery. The result is a product with a spatial detail of 1-meter colorized with information from the multi-spectral data.

This trend is creating headaches for the US. As the Vice-Commander for US Air Force Space and Missile Center, Los Angeles Air Force Base said, "Commercial satellites will increase the amount of information available to US forces. At the same time however, it will increase the amount of information that can be used against the American forces and allies."[36] But it is not just the volume and clarity of the pictures that is worrisome. The speed of delivery of the picture is becoming a national security problem.

Timeliness of satellite imagery is also dramatically improving. Previously Russian satellite imagery of 1-meter resolution was available no sooner than nine days after it is shot. Now Space Imaging's IKONOS satellite constellation can revisit nearly any spot on Earth every three days at 1-meter resolution and every day at lower resolutions.[37] It can get a preliminary image out as quickly as 30 minutes after the shutter snaps.[38] Five day old images qualify as archival and sell for $30 to $300 per square mile of mapped surface on the company's web site, www.spaceimaging.com.[39] If Space Imaging's two American competitors, Orbital Imaging Corporation and Earthwatch, stay on their launch schedules 1-meter visibility could reach once a day within a year.[40]

Concern over the improving resolution and timeless of commercial satellite imagery has caused some governments to begin placing controls on remote sensing. US Presidential Decision Directive 23 (issued in 1994) includes a provision that the US has the right to limit the collection and distribution of high-resolution imagery that might damage national security.[41] This "shutter control" directive applies only to systems licensed for operation in the US. France has a similar position. They limit the sale of high-resolution imagery from the French owned Helios-1 satellite to friendly governments and further stipulate that the French government can shut down the system in case of national emergency.[42] But not all nations have similar policies. Israel, for example, is considering launching additional EROS-1 satellites for customer use and providing them with 100 percent control within a geographic region.[43] The West Indian Space Ltd., Cayman Islands, a joint US and Israel venture, has no restrictions on the sales of its one-meter images.[44] Realistically then, there is no oversight control, but rather a commercial supply-demand marketplace where anyone can get a high-resolution photo.

Jeffery Harris, of Space Imaging, argues that third party sales are very real and can dilute the effectiveness of "shutter control."[45] Unless all the nations that fly imaging satellites are willing to agree to the same sort of restrictions, the US will be imposing restrictions while others will be "snapping and selling away." Marketplace supply and demand will rapidly erode the government monopoly on satellite remote sensing or drive US companies out of business because of their inability to compete.

Space-Based Navigation. Another area of satellite development that increases transparency is the US Global Positioning System, or GPS. GPS is rapidly becoming a de-facto world navigation and timing standard. It was developed by the US Air Force over two decades ago to provide precise time and location data to military users 24 hours a day, every day. During the Gulf War, it provided military commanders with navigation data critical to both moving troops and targeting munitions. Since it's rousing success during the War, GPS has been integrated more fully into military operations. By 2002, military planners expect all troops to carry GPS receivers. Precision guided munitions were used four times more in Operation Allied Force than were used in Desert Storm - and that number is constrained only by the limited numbers of precision weapons in US inventory.[46] By 2008, as part of the Joint Direct Attack Munitions (JDAM) program, the AF will have installed GPS guidance kits on nearly 90,000 gravity bombs.[47] Other GPS guided weapons coming on line in the next ten years include Joint Stand-Off Weapon (JSOW), modified Conventional Air Launched Cruise Missile (CALCM), Tomahawk Land Attack Missile (TLAM) and new systems such as the Joint Advanced Air to Surface Missile (JAASM) and the Wind Corrected Munitions Dispenser (WCMD).

GPS is irresistible in the commercial marketplace as well. According to the Department of Commerce, the civilian sector has leveraged the Pentagon's $10 billion investment in technology infrastructure into a market for hardware, software, and services that is expected to grow to $8 billion annually and perhaps $16 billion by 2003.[48] In fact, industry observers estimate that military users account for only 1.5% (and declining) of the GPS market.[49] It is available in automobiles and trucks to aid travelers in navigating unfamiliar interstate exchanges and city streets, to hikers navigating new terrain, to survey and construction crews precisely locating points to centimeter accuracy, to shipping companies to maintain delivery schedules, to police and emergency medical services departments to determine the closest source of assistance for people in need.

The same method it uses to make position measurements also makes GPS an extremely accurate timing system. A new, important dual use GPS application is its intrinsic precise worldwide timing. GPS is the only technology today that can typically provide an accuracy of 50 nanoseconds or greater over intercontinental distances. [50] This is useful in many industries worldwide. It is used in communication systems to synchronize the transmission of cellular phone messages and of signals from pager network towers, where a unique time signal tags each call to ensure that it is routed and transmitted properly. GPS timing synchronizes power plant generators to provide electrical phase matching and fault detection throughout power grids in the United States.[51] Investment bankers also use GPS to timestamp trades on international networks to ensure that interest income calculations are based on proper dates and time. The number and variety of GPS uses continues to grow.

GPS dual use poses problems for the military. First, commercial users are employing local "augmentation" services to provide more accurate location data, by correcting the built in error the military put into the civilian GPS signal, than GPS or even encrypted military GPS signals can provide. (This augmentation system uses a base station with a known location to beam an additional signal to commercial GPS users.) Secondly, GPS is becoming an international navigation standard. In 1996, President Clinton committed the US to provide nonmilitary use of GPS on a *continuous*, worldwide basis, free of direct-user fees.[52] Although the United States wants to prevent enemy use of GPS during wartime, national US policy dictates the Air Force must operate GPS as a "global information utility" without unduly disrupting or degrading civilian uses of the system. This was reinforced in a recent bilateral cooperation agreement with Japan; the world's other leading producer of GPS equipment.[53] In addition, the presidential policy includes a provision that the president will make an annual determination on whether the military can continue to selectively degrade the accuracy of the GPS signal from 16 to

100 meters. This has become a contentious issue for the military, as many people in the national security field believe it will be discontinued before the 2006 deadline.[54]

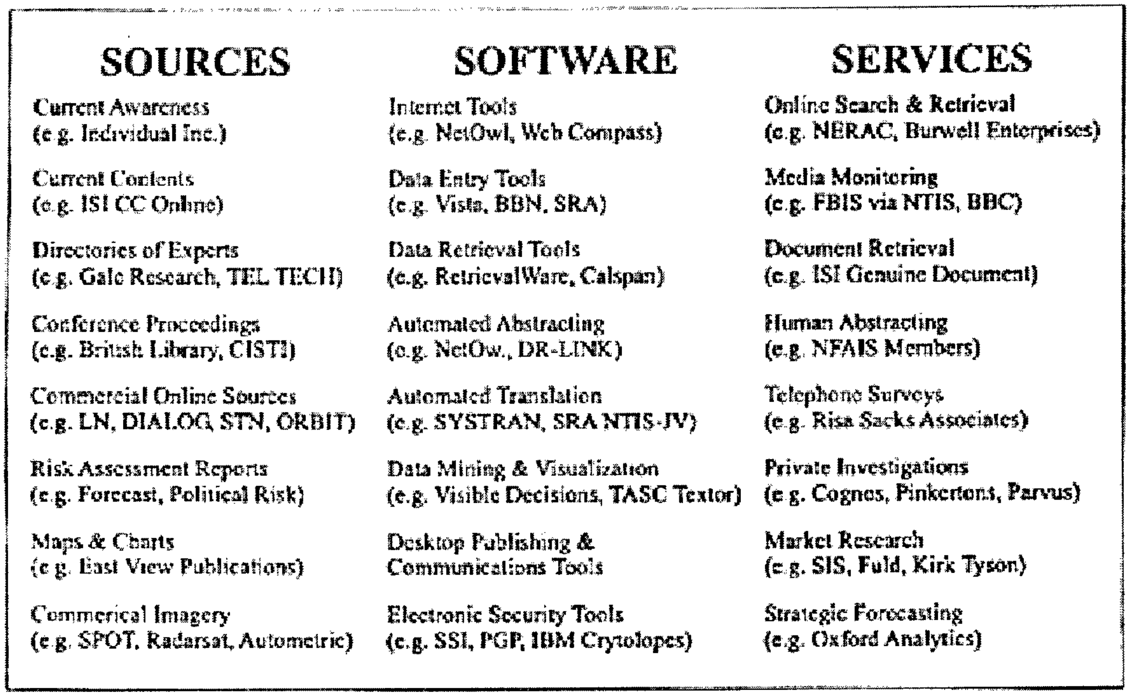
To the US military, commercial GPS service represents a dangerous diffusion of military capability. After all, GPS is what provides the low cost precision guided missile its accuracy. With this increasing technology diffusion, shoot-to-coordinate accuracy may no longer be a US monopoly. According to several studies, including one by The Critical Technologies Institute, potential adversaries could use GPS for cruise missile guidance.[55] In fact, China is already employing a combination of GPS and GLONASS (the Russian navigation equivalent) receivers in an integrated navigation system for their ballistic missiles. The robust combination of GPS/GLONASS aiding improves overall missile accuracy by more than 25%. As an additional targeting aid, the Chinese are integrating GPS/GLONASS into their mobile launchers to further enhance the initial reference point and increase accuracy.[56] For the US military, GPS is a two edged sword – an ambivalent commodity in time of war that can be used against us as much as for us.

National Security considerations may become overwhelmed by irresistible "commercialize space" market forces. The US military must therefore take a serious look at the products provided by commercial satellite systems. Many of these products, from imagery to communications to navigation, are excellent and cost-effective tools a military - one's own or a potential adversary's – can use. The US military must evaluate the value of this dual use asset on the way its military and its adversaries will fight.

Internet: The Information Superhighway

Another key contributor to transparency is the Internet. Within the last five years, Internet traffic has grown 86% per year, more than six times the growth of voice traffic.[57]

In June 1998, Matrix Information and Directory Services (MIDS) reported that there are 102 million people accessing the Internet worldwide.[58] MIDS estimates that the total number of worldwide Internet users will grow to 707 million by 2001.[59] In essence, information access has become unlimited. Over 205 countries have at least one connection to the Internet.[60] All it takes is a personal computer connected to the Internet and one can search massive amounts of information rapidly and systematically for technical and human intelligence information. Figure 2 shows an illustrative, but by no means comprehensive, range of open sources, available software and on-line research services to help people locate any and every thing.[61]



SOURCES	SOFTWARE	SERVICES
Current Awareness (e.g. Individual Inc.)	Internet Tools (e.g. NetOwl, Web Compass)	Online Search & Retrieval (e.g. NERAC, Burwell Enterprises)
Current Contents (e.g. ISI CC Online)	Data Entry Tools (e.g. Vista, BBN, SRA)	Media Monitoring (e.g. FBIS via NTIS, BBC)
Directories of Experts (e.g. Gale Research, TEL TECH)	Data Retrieval Tools (e.g. RetrievalWare, Calspan)	Document Retrieval (e.g. ISI Genuine Document)
Conference Proceedings (e.g. British Library, CISTI)	Automated Abstracting (e.g. NetOw., DR-LINK)	Human Abstracting (e.g. NFAIS Members)
Commercial Online Sources (e.g. LN, DIALOG, STN, ORBIT)	Automated Translation (e.g. SYSTRAN, SRA NTIS-JV)	Telephone Surveys (e.g. Risa Sacks Associates)
Risk Assessment Reports (e.g. Forecast, Political Risk)	Data Mining & Visualization (e.g. Visible Decisions, TASC Textor)	Private Investigations (e.g. Cognos, Pinkertons, Parvus)
Maps & Charts (e.g. East View Publications)	Desktop Publishing & Communications Tools	Market Research (e.g. SIS, Fuld, Kirk Tyson)
Commerical Imagery (e.g. SPOT, Radarsat, Autometric)	Electronic Security Tools (e.g. SSI, PGP, IBM Crytolopes)	Strategic Forecasting (e.g. Oxford Analytics)

Figure 2 Open Source Niches

Web search engines can enable one to find out virtually anything. For example under the auspices of the Air Force Space Command, Space Warfare Center, Aggressor

Space Applications Project, a "red cell" was formed to see if it could, using only open-source information and commercial satellite imagery, track the deployment of an Air Expeditionary Force (AEF) to Bahrain in October 1997.[62] Without any special Internet access privileges to "mil" sites, the Red Cell quickly learned a great deal about the AEF deployment. They discovered where the AEF would deploy, its mission, and its force composition. The team tasked the French SPOT satellite to image the AEF bed-down locations in Bahrain, as well as Mountain Home Air Force Base, Idaho.[63] Image analysts located the AEF headquarters, hardened aircraft shelters, refueling areas, and the "Tent City" for deployed personnel.[64] Clearly the Red Cell pieced together a valuable intelligence picture using a combination of open source Internet references and commercial satellite imagery.

But the Internet can distribute this information – or any other type– to anyone, including someone with little experience in working with search engines. With a Pentium-class PC, a graphics program, image processing software, and an Internet connection, anyone anywhere can buy and manipulate high-resolution imagery for an investment less than $10,000.[65] If you don't know anything about satellite images, one can use a web browser. For example, typing in "satellite imagery" in the search block for "askjeeves" will direct you to numerous web site addresses including http://ourworld. compuserve.com/homepages/mjff/sources.htm. for detailed sources of satellite photographic imagery and imaging radar, or www.satellite.eu.org/sat/vshop, for a catalog of visible satellites, their positions, and orbits. If you don't want a satellite to see what you are doing, you can use it to determine when the satellite will be passing overhead and then deceive or deny the satellite sensors the correct information. For example, it was alleged that Indian workers at the Indian Nuclear Testing Grounds were moved out of view to avoid being seen during passes by overhead US satellites. The US was thereby caught unaware when India recently tested their nuclear weapon.[66] If you are a little more Internet versant and ready to purchase satellite imagery try:[67]

Focal Point GeoGraphics at http://208.228.111.128/avhrr.html

Microsoft's TerraServer at http://www.terraserverr.microsoft.com

Earth Observation Data Services, Dornier Satellitensysteme GMBH at http://www.observe.de/geoids/geoshop.cfm

SPOT Image at http://www.spot.com

Availability of imagery to an adversary is only half the problem – the other half is the availability of trained photo interpreters to extract useful information from the imagery. A brief search on the Internet revealed at least twenty different individuals and companies advertising imagery analysis services. There are at least one on-line aerial photo interpretation tutorial and numerous catalog extracts for university-level photo interpretation courses. A brief representative sample of web sites advertising imagery interpretation services and training includes:[68]

Pinpoint Geographics Inc at http://pinpointgeographics.com/index.html

Sereda Engineering Co. at http://enviroenterprise.com/sereda/html

Fleximage at http://fleximage.fr/indexa.htm

The Internet provides more militarily useful information than just satellite imagery. The web offers many sites that will provide specific military items like camouflage and concealment netting. Companies, like Barracuda, develop frequency-reflecting camouflage nets to hide objects such as tanks and armored personnel carriers from satellites. If it exists, it is likely to be out it there on the Internet.

To make the issue more difficult, recent web technology advancements allows for the concealment of an individuals Internet addresses. Montreal Canada Zero-Knowledge Systems Inc has launched a new service that lets people remain completely anonymous while sending e-mail, visiting Web sites, or making purchases over the web.[69] It allows individuals to hide not only identities but also their trail across the Internet.

The summary the Internet is like a "super-library", open to all, twenty-four hours a day with relatively no restrictions. Imagine the impact as the Internet is combined with another wealth of readily available information, the rapidly evolving 24-hour information news networks.

Worldwide Media Coverage

Continuous TV news coverage can provide potential adversaries military assessments more timely than traditional military intelligence analysis. While these capabilities have always been targeted and known to some degree, the information they are beginning to provide is intentions. In open democratic systems such as the United States, the reasons and meaning of US actions will increasingly be discussed publicly. Secrecy is becoming rare.

Traditionally, the media is obligated to protect vital military secrecy while seeking out stories to fulfill the "people's right to know." However, the competitive pressure on the media to have the best, freshest news, as exemplified by their rating system, has in the past twenty years produced situations that bolster the US military's "doubt about the trustworthiness of reporters." A person in a key position in American media recently said, “It’s not my job to keep your secrets; if I get one, and it’s a good story, I’m going to have to print it.”[70] In 1999, during a Columbia University Seminar on Media and Society, ABC News Anchorman Peter Jennings and CBS News Anchorman Mike Wallace were challenged on a moral dilemma of reporting the news or saving American soldier lives. After agonizing, Peter Jennings said he would help the Americans while Mike Wallace said he would report the news. “There is no higher calling.”[71] This is a particularly challenging question as the American media becomes less American and other nationalities join their ranks. CNN epitomizes an emerging electronic life-form that is slowly becoming the eyes and ears of the world community.[72]

A new tool of continuous TV news is the use of commercial satellite imagery and knowledgeable consultants to inform the American public, and the rest of the world, of late breaking news on the why, how, and when of US military deployments. The proliferation of “all news” networks like the Cable News Network (CNN), Skynews, and others impact political and military actions. CNN reporting of the infamous “Highway of Death” was followed closely by the Coalition’s announcement of a cease-fire is a reminder of the principle that political considerations permeate war. Another example is the sharp reduction of coalition air strikes against leadership targets after the destruction of the Al Firdos bunker in the fourth week of the Persian Gulf war. Coalition target planners had no prior indication (before seeing post-strike television coverage over CNN) that this legitimate military target had been occupied by civilians.[73] After the report, General Schwarzkopf implemented a policy wherein he personally reviewed any target selected for air attacks in downtown Baghdad. Those images decisively altered our operational and strategic goals.[74]

Decision-makers find themselves increasingly considering not only actual media coverage of events such as air attacks on Iraqi's trying to flee the Kuwait theater, but *anticipating* coverage of such events.[75] RAND recently asserted that the Cable News Network (CNN) appears to be more pertinent than CIA Intelligence Estimates for current White House decision making.[76] The significance of continuous network news is that it represents information that is immediately available to the public (e.g., daily briefs, Internet sites, etc). Furthermore, the convergence of near-real time commercial imagery and leased commercial communications satellites with 24-hour news media increase the influence of the media. [77]

CNN, by default, can influence the political, and hence the military agenda of a nation.[78] The military affectionately call this the "CNN effect" because of their indelible impression that global, real-time news coverage makes the conduct of most military operations a matter of immediate public scrutiny.[79] The military's rapid pullout from Somalia may be attributed to the CNN effect. The American government was compelled to reassess its policy when CNN and others broadcast their power images of a naked dead Marine being dragged through the streets of Mogadishu, Somalia. Furthermore, continuous coverage news organizations like CNN are great, open source, intelligence assets when they broadcast real-time satellite imagery of US deployments or coalition actions. Examples of these include the US Marines amphibious landing at Mogadishu and the coalition strike aircraft departures from Aviano Air Base, Italy during Operation Allied Force. An adversary could mine the Internet for data and news media for intentions, create hypotheses, and then use commercial satellite imagery to evaluate and access possible US courses of action. Internet access, competitive space-based remote sensing and twenty-four-news coverage are all converging to make it exponentially harder for military operations to be kept secret.

Chapter Summary

Military information transparency seems inevitable. It is the result of worldwide economic globalization, the dual use nature of new technologies and the shift of new technology development from military to commercial sponsorship. The explosive advancements in commercial remote-sensing, navigation and communications space systems, Internet access and powerful Internet web search engines and access, and global coverage of continuous news all point towards the evolving age of transparency. This diffusion will impact the nature of war. The US military needs to recognize this trend and asset its impacts.

The following chapter investigates how transparency affects warfare. It begins by looking at the impact information technology diffusion has on the principles of war. It then looks at how this diffusion impacts two preferred late 20th century American ways of war – traditional coalition warfare and use of technology as a force multiplier.

Notes

[4] Florini, Ann., "The End of Secrecy", *Foreign Policy*, Summer 98, Issue 111, p. 63.

[5] Carus, W. Seth, "Military Technology and the Arms Trade: Changes and their Impact," *Annuals of the American Academy of Political and Social Science*, Sep 94, Vol. 535., p. 169.

[6] Carus, p. 167

[7] Peters, Katherine McIntire, "Space Wars", *Government Executive*, April 98, Vol. 30, Issue 4, p. 13.

[8] Johnson, Dana J. and Scott Pace, and C.Bryan Gabbard, *Space: Emerging Options for National Power*, RAND, 1998, p. 37.

[9] Moorman, General Thomas S., USAF Retired, "The Explosion of Commercial Space and the Implications for National Security," *Airpower Journal*, Spring 99, Vol. 13, Issue 1, p. 6-21.

[10] Lantz, Terry D., Mobile Satellite Services", http://doserve.mall.nsa.ic.gov/producer/ttn/8-2/mobile.html

Notes

[11] See http://www.tcmet.com/tcmet/newsit/H1000249.htm

[12] Ibid.

[13] Johnson, Dana J. and Scott Pace, and C.Bryan Gabbard, *Space: Emerging Options for National Power*, RAND, 1998, pp. 25.

[14] Ibid, p. 25.

[15] Ibid, p. 25.

[16] Moorman, S. (Gen), "The Explosion of Commercial Space and the Implications for National Security", *Airpower Journal*, Spring 99, vol 13, Issue 1, p. 10.

[17] Lantz, Terry D., "Mobile Satellite Services, ", Oct 25, 1999, http://doserve.mall.nsa.ic.gov/producer/ttn/8-2/mobile.html

[18] Black, J. Todd, "Commercial Satellites: Future Threats or Allies?", http://www.nwc.navy.mil/press/Review/1999/winter/art5-w99.htm

[19] Fuller, Andy, "Inmarsat Maritime Services and Products," Inmarsat Facts, January 1997, http://www.inmarsat.org/inmarsat/html/media_supp/factsheets/maritime.pdf.

[20] Myers, Richard B (Gen)., Investment in Space, *Air Force Magazine, February 2000,* p. 51.

[21] Ibid. p. 24.

[22] As a rule, countries (besides the US, Russia, and UK) that wish to have a military presence in space will usually opt for dual-use satellites, which carry both military and commercial transponders. Ibid, p. 25.

[23] Television companies like CBS regularly use two-meter resolution imagery in news bulletins. Red Lemon, a Glasglow Ireland computer game manufacturer, used Russian developed satellite mapping of Scotland for its most recent game, Braveheart.

[24] Tahu, George J. and John C. Baker, "Expanding Global Access to Civilian and Commercial Remote Sensing Data," *Space Policy*, Aug 98, Vol 14, Issue 3, p. 188.

[25] "Eyes in the Sky a Growing Concern," http://www.space.com, 17 Mar 2000, pp. 20.

[26] Policy Makers not ready for Commercial Imagery," Defense News, Issue XX, April 3, 2000, p.1.

[27] Tahu, George J. and John C. Baker, "Expanding Global Access to Civilian and Commercial Remote Sensing Data," *Space Policy*, Aug 98, Vol 14, Issue 3, p. 179.

[28] "Policy Makers not ready for Commercial Imagery," Defense News, Issue XX, April 3, 2000, p.1. See Also "Eyes in the Sky a Growing Concern," at http://www.space.com, 17 Mar 2000, p. 19.

[29] Verton, Daniel and L. Scott Tillett, "Commercial Imagery Prompts NIMA Doubts," *Federal Computer Week*, Oct 18, 1999. Also at http://www.fcw.com/pubs/fcw/1999/1018/fcw-newsnima-10-18-99.html.

[30] Wright, Robert, "Private Eyes," *New York Times Magazine*, Sept 5, 1999.

[31] Anselmo, Joseph C., "Commercial Space's Sharp New Image," *Aviation Space and Week,* Vol. 152, No. 5, January 31,2000, p 56.

[32] Israeli EROS (previously a military system, now commercial) boasts a one-meter resolution in some applications. The stated goal for the next launch is 1.5-meter resolution. "Eros Partners Will Modify Ground Stations for Free," Space News, February 18, 1997. See also http://www.coresw.com/news/sn19970218.html

Notes

[33] Ibid.p.122.

[34] "SPOT 5 Improvements Reflect Policy Shift," *Space News*, February 12, 1997. See also http:www.coresw.com/news/sn19970212.html

[35] Amato, Ivan, "God's Eyes for Sale," Mar/Apr 99, Vol. 102, Issue 2, pp. 36.

[36] "US Officials See Pros and Cons in New Imaging Satellites," *Space News*, 7 Nov 99.

[37] Crawley, James W., "Satellite is looking at you, kid," *The Arizona Republic Newspaper*, pp. E1.

[38] Wright, Robert, "Private Eyes," *New York Times Magazine*, Sept 5, 1999. See also http://delphi.dia.ic.gov/admin/EARLYBIRD/990907/s19990907private.html.

[39] Wright, Robert, "Private Eyes," *New York Times Magazine*, Sept 5, 1999. See also http://delphi.dia.ic.gov/admin/EARLYBIRD/990907/s19990907private.html.

[40] Ibid.

[41] The White House, Office of the Press Secretary, "Statement by the Press Secretary," 10 March 1994. Also at http://library.whitehouse.gov/Search/Query-PressRelease.html.

[42] Gupta, Vipin, "New Satellite Images for Sale," *International Security,* Summer 1995, p. 94.

[43] Gutpa, Ibid, p. 104.

[44] Wright, Robert, "Private Eyes," *New York Times Magazine*, Sept 5, 1999.

[45] Foreman, Tom, " Satellites are Watching You," ABC World News Tonight, Jan 17, 2000. See also www.abcnews.go.com/onair/WorldNewsTonight/wnt_000113_CL_satellites_features.html

[46] Cordsesman, Anthony H., "*The Lessons and Non-Lessons of the Air and Missile Campaign in Kosovo",* Center for Strategic and International Studies, Sept 29, 1999, pp 21.

[47] Newman, Richard J., "The New Space Race," *US News and World Report*, November 8, 1999, p. 36.

[48] Martello, Norman, "Where in the World," *Electric Perspectives*, Mar/Apr 99, Vol 24, Issue 2, p. 14

[49] GPS Industry Council, 1996

[50] Martello, Norman, "Where in the World," *Electric Perspectives*, Mar/Apr 99, Vol 24, Issue 2, p. 16.

[51] Ibid. p. 18.

[52] Fact Sheet, the White House, Office of Science and Technology Policy and National Security Council, subject: US Global Positioning System Policy, 29 March 1996.

[53] The White House, Office of the Press Secretary, "Joint Statement by the Government of the United States of America and the Government of Japan on Cooperation in the Use of the Global Positioning System," 16 September 1998.

[54] Moorman, p.16.

[55] Sewell, Kelly, "Sensor Integration Placing GPS Devices on Center Stage," *Military & Aerospace Electronics*, May 96, Vol 7, Issue 5, p. 25.

Notes

[56] Stokes, Mark A., *China's Strategic Modernization: Implications for the United States,* Strategic Studies Institute, September 1999, p. 92.

[57] Global Crossing Fact Sheet. http://globalcrossing.com/network.asp

[58]International Cmmunications Headcount.com. www.mids.org/mmq/501/pages.htm

[59] Ibid, www.mids.org/mmq/501/pub/ed.html

[60] Ibid

[61] Matthews, Lloyd J., "Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated?", US Army War College, 1999, pp. 158.

[62] US Air Force Space Command, Operation SEEK GUNFIGHTER – Aggressor Space Applications Project Operational Report (Colorado Springs, CO: Falcon AFB, 23 January 1998), p. 24.

[63] Ibid, p. 4.

[64] Ibid, p. 7-15.

[65] "Countering the Threat Posed by Commercial Satellite Imagery (U)", AF/XOI White Paper, 15 March 1999, p. 13.

[66] Newman, Richard J., "The New Space Race, The Pentagon envisions a war in the heavens but can it defend the ultimate high ground?" *U.S. News and World Report*, November 8, 1999, p. 30.

[67] "Countering the Threat Posed by Commercial Satellite Imagery (U)", AF/XOI White Paper, 15 March 1999, p. 13.

[68] "Countering the Threat Posed by Commercial Satellite Imagery (U)", AF/XOI White Paper, 15 March 1999, p. 14.

[69] Kalish, David E., "Your Secret E-Mail Service," Dec 13, 1999, ABC News. See also http://more.abcnews.go.com/sections/tech/dailynews/internetsecrecy991213.html.

[70] Steinberg, Stephen, "Travels on the Net," *Technology Review*, July 1994: p. 22-30.

[71] Columbia University Seminars, Media and Society, Ethics in America: "Under Orders, Under Fire, p. 4.

[72] Kaplan, Robert D., "Fort Leavenworth and the Eclipse of Nationhood," *The Atlantic Monthly*, Vol. 278, No. 3, September 1996, pp. 81. SEE Also DFI reader p. 50.

[73] GWAPS, p. 69.

[74] Toffler and Toffler, *War and Anti War: Survival at the Dawn of the 21st Century,* Little Brown and Company, 1993, p. 67

[75] GWAPS p. 251.

[76] Cooper, Jeffrey, "*Another View of the Revolution in Military Affairs,*" Strategic Studies Institute, US Army War College, 15 July 1994.

[77] Grundhauser, Larry K. "Sentinels Rising", *Airpower Journal*, Winter 98, Vol. 12 Issue 4, p. 67.

[78] Builder, Carl H., *The Icarcus Syndrome*, Transaction Publishers, New Brunswick, p. 249.

[79] Cooper, Jeffrey R., *Another View of the Revolution in Military Affairs,* 15 July 1994, p. 45.

Chapter 3

Transparency and the American Ways of War

Our enemies have seen CNN. They watched the technology and they will not be content to fight the son of DESERT STORM. They will fight the stepson of Chechnya, the stepson of Allied Force in Kosovo.

General Charles Krulak
United States Marine Corp

As the nearly unavoidable result of the globalization of our economy, our open society, and the evolving dual use nature of military and commercial technology, the US military veil of secrecy is becoming far more transparent. In fact, the US faces acceleration in the pace and scope of the transparency process. The explosive advancements in commercial space systems with remote sensing, telecommunications, and navigation, Internet access, and global continuous is creating a transparent world. The challenge to the US now is to assess how future military operations will be impacted by this transparency and evolve effective responses.

Throughout the history of conflict, military leaders have noted certain principles that tended to produce military victory. These "truths" have served as the cornerstone of military thinking in different centuries, for different armies, under different strategic conditions to achieve various goals by means of force. Known as the "principles of war," these aspects of warfare are considered universally true and relevant.[80] The first US exposition on the "principles of war" appeared in the War Department Training Regulations No. 10-5 of 1921. Since then few changes have been made to the nine-item list. Today's list includes all the current principles – objective, offensive, mass, economy of force, security, surprise, and simplicity, with maneuver and unity of command replacing movement and cooperation respectively. The fact that very few changes have been made over the last 80 years indicates the consistency, validity, and applicability of these principles of war to each of the four Services.

The US military has been integrating information technologies into its operations for the last ten years. It now greatly depends on computers, computer networks, and high-speed communications.[81] Consequently, the principles of warfare must be considered in light of the realization that the possession and manipulation of information itself can be a key element of the warfare. While information manipulation via ruses, stratagems, and deception has always been a part of warfare, the increasing diffusion of information technology into an international world, and its increasing relevance to warfare makes the following assessment even more critical. Information itself is now, in many cases, a weapon or target.[82]

This chapter investigates how information transparency is changing the American ways of war. It will begin by first investigating the impact transparency has on the nine basic principles of warfare. It then shifts perspective and look at how transparency impacts US preferences for coalition warfare and using technology as a force multiplier.

Impact on the Principles of War

Many countries are using transparency to developing asymmetrical responses to the widening gap between their conventional capabilities and those of the United States.

While they realize they cannot compete in the arena of conventional western style warfare, they can selectively exploit commercial sources to compete asymmetrically, and they do.

In the Army After Next as well as OSD's Net Assessment war games, asymmetrical responses characterized the Red Team's reaction to Blue's superiority in firepower and information dominance. "Red's learning curve rose sharply as the games progressed. Confronted by overwhelming combat power, Red resorted to asymmetric responses in an effort to offset Blue's advantages."[83] Their goal was simple: deter US intervention in a regional conflict, otherwise make US involvement as costly as possible. Their only way to achieve this was to develop strategies and acquire selective technologies to offset the US advantages. Therefore it is important to look at how transparency impacts the principles of war. Interspersed in the discussion that follows, hypothetical examples are provided of how an adversary could asymmetrically exploit transparency to deny the US's ability to successfully apply its principles of war.

Principle of War #1 - Objective. "Direct every military operation towards a clearly defined, decisive and obtainable objective that contributes to strategic, operational, or tactical aims."[84] In application, this principle refers to the unity of effort, directing all efforts to achieving a common goal. From an airman's perspective, this principle shapes priorities to allow air and space forces to concentrate on theater or campaign priorities. It also seeks to avoid siphoning off force elements to support fragmented objectives. Information technology serves as an enabler for obtaining better-defined, clearer objectives. The clarity and speed (i.e., celerity) at which the data is provided to the appropriate players also creates a self-feeding demand for more information and more communications delays as the people wait for their need to be filled. Transparency may negate this "waiting-for-more-data" delay syndrome as commercial sources may be used to fulfill some of the information need. Web browsers can be used to filter information or provide a common "chat room" for discussion.

But conversely, transparency may indirectly work against the US military. Whatever commercial tools used are undoubtedly available to our adversaries. They can use commercial communication and remote imaging satellites with inconsistent international "shutter controls," Internet access with associated data mining technologies, and continuous news reporting. They can garner information about US military troop locations, equipment deployments, and political and military objectives (from interviews of US officials and "expert guest" commentaries). An adversary can then piece together carefully collected open source information, including railroad traffic movement, ship movement, air traffic control display information, business parts orders, and pizza deliveries to the Pentagon. All of this could be collected from the Internet and twenty-four hour news sources, confirmed via satellite imagery, analyzed using commercial advancements in database technology to discern possible US objectives, and used to generate indications and warnings of their implementation. Knowing US objectives and intentions will make it easier for an adversary to develop a successful countervailing strategy and objectives.

<u>Principle of War #2 - Offensive.</u> "Seize, retain and exploit the initiative. Dictate the time, place, purpose, scope, intensity, and pace of operations: Act rather than react."[85] To air and space forces this means to control the air and space. To information warriors, this means to control the flow of information, achieve information dominance. But how can

one attain the initiative when in the future an enemy can monitor US actions using commercial information systems? Transparency makes both offensive surprise and target selection harder to achieve. In a regional conflict scenario, an adversary would detect the initial deployment and initiate immediate evasive actions to offset the attack. Furthermore, his previous judicious uses of deception and denial techniques would have made it difficult for US target analyses' to develop robust targeting folders. In short the effect of transparency is heightened awareness of the compelling need to maintain secrecy of action. But transparency impacts more than just tactics.

Defense analyst Dr. Jeffrey Record has asserted that American forces were stalemated in Korea, defeated in Vietnam, and humiliated in Lebanon and Somalia when their opponents *took* the strategic initiative and forced the kind of fight where high firepower and air power could not be used effectively.[86] The French experience in Indochina and the Soviet experience in Afghanistan were similar.[87] In each case, the adversaries chose not to fight "western style" but rather in their own cultural styles. In the age of increasing transparency and national desire to localize or contain conflict – with no casualties, so that economic growth and democracy continue to spread, the dialectic will continue to be at work. A competent adversary could construct a situation wherein the US is forced to fight a fight where information systems are deliberately misled with misinformation and hence a strategic vulnerability. He could reduce or even eliminate any supposed advantages in information age warfare in a number of ways.[88] He may purchase off the Internet Russian *maskirovka* techniques and camouflage equipment in an effort to overwhelm our information collection systems with invalid information. He could also limit the effectiveness of our collection systems by constructing redundant fiber optic based command and control infrastructures. This hardwired system would be much more difficult for the US military to destroy. The net result to US forces would be a more difficult time in prosecuting the war. This is particularly troublesome since the US military has adopted a stance that it will use information technology to offset the shrinking force structure; the specific phrase is "employing just the right amount of combat power at the right time at the right place." Consequently, any strategy that the US develops that does not anticipate transparency and plan counter-strategies will leave the nation unnecessarily vulnerable.

Principle of War #3 - Mass. "Concentrate combat power at a decisive time and place."[89] For airpower, the definition of massed forces has changed with the advent of precision weapons. No longer do aircraft have to fly in mass formations to strike a target; today it is one platform launching a few precision guided munitions to achieve the desired damage. In essence, mass is in the effects achieved, not the means to obtain them. With superior battlespace awareness and targeting, a single precision guided weapon can cause the target destruction that in the past took hundreds of bombs. As a result, campaign plans have become carefully orchestrated events designed to support the weapon releaser. Strike packages, composed of escort jammers, stealth and conventional fighters and bombers, and tanker escort, supported by theater Intelligence, Surveillance and Reconnaissance (ISR) and C3I platforms, must all be tightly choreographed and synchronized together to perform their specific function - at the designated time - for the overall strike mission to be effective. If the events do not unfold as specified, aircraft/pilots are at risk of being shot down.

Transparency will require strike planning to take on a new perspective. The adversary may use transparency to determine where forces are originating from and massing. They could construct a way to degrade that bases capacity either physically or politically. For example, adversaries could use their own high revisit rate satellite imagery or Internet purchased commercial imagery to evaluate US forward basing locations and activity. They could them employ commercially purchased night vision equipment to detect the inbound night attack, and position GPS jammers or spoofers near high value targets to degrade the US military's tactical communications and precision munitions effectiveness. Also since the US military uses fewer strike sorties and fewer precision munitions to achieve the same lethal effect (i.e. effects based targeting), it may no longer be necessary or desirable for the US to mass as many strike platforms over the objective. Even more importantly strike aircraft, through theater-wide strike synchronization, could operate from many smaller and distributed forward-operating bases. The US may have to evolve its strike planning, operational tactics, and logistics to disperse combat power in time and space over the attack zone and as well as further mask its support activity from view.

Enemy Example: Deny US access to theater. Two preconditions that enable US forces to possess the strategic agility, overseas presence, power projection, and decisive force capabilities essential to defeat aggression are adequate time to deploy US forces overseas and unobstructed access to theater seaports and airfields. If either or both are degraded or denied by an asymmetric enemy, the existing US national military strategy is less effective. An intelligent potential enemy would seek to deny these capabilities using his diplomatic, economic, military, and political instruments of national power to actively delay, disrupt, or block US forces from deploying into theater.

In Desert Storm, Americans and potential future adversaries (re)learned just how long it takes to deploy large numbers of forces (ships, planes, and troops) to the theater of conflict. Clearly in future conflicts, the time to deploy forces overseas will become a perishable commodity. The longer it takes for the US to decide whether and how it will engage, the more advantageous it will be for an adversary. Department of Defense studies state that US forces must have at least two weeks of actionable warning and uninterrupted deployment time. If the warning and deployment time is less than two weeks, or if the adversary starts shooting before US forces are fully deployed and in place, significant military risk could result.[90] To this end, future adversaries will exploit transparency to gain several advantages.

In the aforementioned Pentagon war games, US forces are typically assumed to have unlimited and unobstructed access to theater ports, airfields, and coastal waters. This assumption may become unwarranted. Due to politically driven denials and internal budget constraints, the US increasingly finds itself losing access to forward bases (down to 14 in 1996), denied over-flight rights and given operational restrictions on the use of overseas bases. A potential adversary should be expected to leverage this US need for host nation support. They could employ coercive diplomatic action to get a skittish potential host country to deny to the US forward basing rights or overflight rights. This would force the US and its allies to operate further away from the conflict zone. This has tremendous secondary affects on the operations tempo. Aircraft would have to stage into the theater of operations from farther away and additional travel time and fuel would be needed for Air Force strike packages to travel to and from their targets. Further complicating matters is the limited numbers of useable airbases, with limited ramp space, for servicing or reloading aircraft with weapons. Lastly, greater numbers of aircrews, maintenance, and support personnel would have to be stationed forward. After all, the longer the distance, the higher the crew ratio needed – for tankers, shooters, C4ISR aircraft etc. - to keep the strike aircraft up performing their missions. All of this decreases sortie generation rates and bombs on target, exposes planes and personnel to more risk, lengthens the campaign, and works against a massive, high technology, short, low casualty war – the kind the US prefers. But sometimes an adversary does not have to use strong-arm tactics.

Politics and geography interact together can constrain US military operations. In 1996 US led forces ended up watching helplessly when Iraqi Republican Guards invaded the UN declared safe haven Kurdish city of Irbil, located about 200 miles north of Baghdad. When Turkey, Jordan and Saudi Arabia decided they would not allow air strikes against Iraq to be launched from within their territories, US options were significantly narrowed. Unable to strike the offending Iraqi Republican Guards in Irbil, the US was forced to strike air defense facilities south of Baghdad with forces that were within range of the target. [91] Coalition sensitivities to the US plan created significant obstacles.

Adversaries could also exploit commercial satellite imagery and communications and the media to influence the US or host nation decision-makers and retard the military decision cycle or tempo of US military operations. They could launch precision guided (cruise or even tactical ballistic) missile strikes using conventional, biological or chemical warheads against airfields and seaports. The enemy could determine when best to launch a strike by data mining the Internet, exploiting commercial imagery to determine movements and monitoring the news media to obtain strategic warning and track US deployments. Alternatively they could use anonymous terrorists or unsuspecting third parties to achieve these objectives. This would be both to punish any country granting US access to its military facilities, seaports or airports and to prevent US forward basing.

Massive disruption of this sort is not novel. In 1943 a German air strike against Allied shipping in the harbor of Bari, Italy demonstrated the effects of weapons of mass destruction (WMD) attacks against seaports. More than 30 ships had choked the harbor waiting to unload, among them the USS John Harvey which was loaded with 2,000 chemical bombs, each with 60-70 pounds of mustard gas. Within 20 minutes the strike force of 105 JU-88 German bombers sank 17 ships and caused several tankers to explode. When the John Harvey was hit, its mustard gas began to burn. Much of it spread throughout the harbor mixing with the tons of oil floating on the water. A mustard gas cloud formed and over 1,000 people died. The port was closed for three weeks and its operational capacity not resumed for two months.[92] This 60-year-old event could be easily replicated today! One could use gas or just an accidental petroleum spill to shut down a major port area. With adversaries desiring to limit US access to the theater of operations, a future country supporting the US could find itself faced with sea mines and submarines off its coasts and direct fire conventional or weapons of mass destruction attacking its ports and airfields. In short, degrading US power projection capability is not that difficult. All an adversary has to do is make the price of access too high for the US and its coalition partners to continue.

US Counter to Enemy Example - Modify Power Projection Strategy. The US Military should look towards negating such a theater denial strategy by modifying its current power projection strategy. A recent RAND report argues that the Air Force needs to rethink where and how it sets up bases near combat zones to better protect its aircraft and people. The report warns that an enemy armed with cheap versions of cruise missiles or ballistic missiles could devastate aircraft parked on unprotected flight lines when the bases are a few hundred miles from the battle zone.[93] Therefore, the Air Force should fund the development of new aircraft protection measures, such as underground shelters (like the rest of the world). Second, the Air Force should examine subdividing its footprint near and around the combat theaters. A distributed mini-basing (vice mega-basing like at Aviano Air Base in Italy during Operation Allied Force) concept should be considered. A concept that can be used to dilute the affects of transparency on basing is discussed in the next chapter.

Principle of War #4 - Surprise. "Strike the enemy at a time, place, or in a manner for which the enemy is not prepared."[94] It is one of air and space power's strongest advantages. Concealing one's capabilities and intentions creates the opportunity to strike the enemy when he is unaware or unprepared. But the increasing transparency created by the proliferation of dual use technologies, modern commercial satellite surveillance technology and warning systems, Internet, and media coverage, can make it increasingly difficult for the US to mask or cloak any large-scale marshaling or movement of personnel and equipment or select the appropriate targets. In short, transparency may seriously jeopardize the military's ability to achieve strategic or tactical surprise, or worse make surprise highly unlikely.[95] The US military may therefore have to change its methodology for achieving surprise.

Transparency also negates tactical surprise. How can the US move or place on alert any forces in secret? Given the increasing reliance on the guard and reserve units, this will be more difficult. Fleet assets are easily trackable. So too, now, are troop and aircraft movements of almost any scale. Add to this the increasing US dependence on contractors for battlefield support and the problems mount. Their deployments and movements could be easily monitored. Surprise will become much more elusive for the US, unless new procedures and methods are aggressively pursued.

Principle of War #5 - Maneuver. "Place the enemy in a position of disadvantage through the flexible application of combat power."[96] The ability to integrate a force quickly and to strike directly at an adversary's strategic or center of gravity is a key theme of air and space power's maneuver advantage. It requires the flexibility, responsiveness, and clarity that information systems provide to support determination of the maneuver plan. Having near-instantaneous situation understanding confers a decided advantage that must be immediately exploited to be of tactical or operational benefit. But with transparency, this can work to the advantage of either friend or foe. It can level the playing field where each player knows what the other is doing. For example, our smaller US Army of today could not accomplish an undetected Desert Storm like left hook and our smaller naval units cannot hide as easily in the vastness of the oceans given the increasing proliferation of space assets and accessibility to information.[97]

Many argue that in retrospect the Gulf War was the last secret war, not the first open modern war. The Gulf War Air Power Survey reports that it may well have been the last war in which only one side had ready access to precise location information from satellites. [98] Information transparency has the potential to level the playing field where each player knows what the other is doing. It is becoming a fact of life that the US military must deal with in a proactive manner.

Principle of War #6 - Security. "Protect friendly forces and their operations from enemy action. Never permit the enemy to acquire an unexpected advantage."[99] Increasingly, there are four areas that must be protected: airpower on the ground (i.e., at airbases), space system ground control elements and telecommunication links to the satellites, logistics facilities, and command facilities to include information centers. These are vital aspects of how the US fights its wars. With the increased dependence on information for battlespace dominance, each pathway that carries intelligence, command information, or relevant data must be protected from being intercepted, tapped or disrupted. But given transparency, this is becoming more difficult.

Just as the Space Warfare Center's Red Cell used the information off the Internet to track the movement of the Air Expeditionary Force in 1997, so could an adversary use commercial information to track US ship or convoy movements, debarkation and embarkation areas, staging and bed-down arrangements, etc. Or an adversary could use commercial data base management and data mining technologies to track and target military activities and gleam US intentions. Ironically, the "pizza index" has been flagged as an accurate predictor of future US military operations.[100] An adversary could set Internet flags to track sharp rises in Domino's pizza delivery to the Pentagon and commercial satellite imagery flags to track Pentagon parking lot occupancy during US combat deployment planning and execution. Thanks to transparency, security will become increasing difficult and cover a broader base of forces.

Enemy Example: Control the War: Degrade US Operations Tempo. The diffusion of information could clearly limit the US's ability to project military power and adequately protect forward bases, particularly if opponents are equally well informed of events in a campaign. An adversary could use the Internet to hypothesize possible US deployment area target portfolios, computing gateways or communications and control centers, airbases, or seaports. They could then launch their surprise attack for limited goals, disperse assets, set out decoys to deliberately confuse overhead and theater sensors, destroy a couple of coalition forward operating bases with tactical missiles, live off pre-distributed supplies in protected locations, and if the US/coalition counter-attacks, force a non-western style of war. As General Fogelman, former US Air Force Chief of Staff, said, "It would make it extremely costly to project US forces in to a disputed region, much less carry out operations to defeat a well-armed aggressor. Simply the threat of such an enemy missile attacks might deter the US and coalition partners from responding to aggression in the first instance."[101]

It is hard to predict what exactly would be the impact of such on US operations tempo, but US actions could be significantly delayed, disrupted, and degraded. China has been paying attention. They now have 17 spy satellites and 40 domestic satellites to continuously track and monitor the global movements of the US military. These satellites could easily be used to guide a "saturated" missile attack on American and Taiwan warships.[102] They are also entering into commercial satellite imaging contracts with non-

US space companies or in joint ventures with other countries to develop an indigenous capability. They have efforts underway with the former Soviet States, France and Germany to gain the knowledge necessary to either launch alone or jointly with others a quality space enhancement capability.[103] They could use these new capabilities to pose a significant threat to the ability of the US to project its military power into the region. In one such fictitious war-game, China, with long range cruise missiles and robust satellite surveillance, inflicted heavy losses on American carrier battle groups.[104]

The adversary could also selectively degrade theater GPS and communications support. A strategic center of gravity of the coalition forces in the Gulf War was their heavy dependence on the orbiting US navigation and communications satellites. For example, if the Iraqis had destroyed Defense Satellite Communication System (DSCS), most of the allied advantage would have dissipated.[105] The dependence on GPS and communications satellites has increased since then. During the war against Serbia, the Pentagon's GPS was essential for guiding precision bombs to their targets in bad weather, maneuvering ships and positioning troops. Therefore an adversary would naturally try to limit the effectiveness of satellite-based communications and navigation within their area of interest.

An enemy could neutralize the GPS signal broadcast from space. They could easily build local jammers to spoof or degrade GPS and commercial satellites in an area, or conduct terrorist attacks on GPS mission ground stations.[106] Hypothetically, China could also deny the US access to its leased commercial communications satellites and supporting ground stations in its Asian sphere of influence. Many possibilities exist for interrupting these communications where the US has no access to prevent denial of service or interception. Without navigation satellites, the US would be denied a common timing and position reference system for targeting munitions. Without communications satellites, the US military could not command and control a distributed multidivisional force.

Either way, in a military bid by China to recover Taiwan, they could preemptively conduct strike missions, area information dominance, command and control warfare and integrated air defense to degrade Taiwan's ability to conduct military operations.[107] In this case of regional dominance, information transparency helps China more than it helps the US. Clearly, the less prepared the US is for an aggressor's actions, the greater will be the strategic impact and the more likely the enemy will be to pursue the needed capabilities to make such an attack plausible. Hence the US must develop new operational level strategies for dealing with the inevitable transparency. But transparency affects aren't just limited to traditional force projection.

However, foreknowledge may not necessarily be translated into effective action. Having 1-meter resolution imagery and CNN expert consultants discussing US deployments does not always mean that an adversary can exploit the information. For example, the adversary may have the fighters to exploit the information, but the aircraft may not be fully equal to or the training of the pilot not as good as the coalition partners or US. More than ever, in the evolving era of transparency, weapon system capability and training in tactics and decision making will make the difference. The quality of people and platforms and the fast-breaking ability to innovate and adapt in combat – at all levels – will be the key to success in future conflicts. This will be discussed more thoroughly in the next chapter.

Principles of War # 7-9 – Simplicity, Unity of Command and Economy of Force: The three remaining principles of war, namely simplicity, unity of command and economy of force are not directly impacted by the evolving military transparent climate. These principles are impacted indirectly depending on how the US works to negate the impact of transparency on the other principles. The impact is unclear. Transparency could support or negate these principles of war.

Simplicity. "Prepare clear, uncomplicated plans and concise orders: avoid unnecessary complexity in organizing, preparing, planning, and conducting military operations." The impact of transparency depends on whether the commander is a micro manager, or the degree of deception, or the number of coalition partners participating. If the manager tracks the details, transparency may produce secondary effects that negate simplicity. In an effort to deceive adversarial commercial satellite imagery, or provide base safety, operational plans could become quite complicated., For example, chaos and parallel effects based warfare might suggest that simplicity is less likely as plans become more complex. On the other hand, if the commander is strictly task oriented, and leaves the details up to subordinate commanders, transparency will have little impact on simplicity.

Unity of Command. "Direct and coordinate all efforts towards a common objective."[108] Unity of command is important for all forces, but it is vital in employing air and space forces. It ensures that the concentration of effort for every objective is under one responsible commander. But can the one commander handle all the information coming at him? Information technology enables commanders to fax, email or video teleconference consult with one another or coalition partners or senior political leadership in near real-time. This transparency supports both sides and senior commanders equally well. Therefore the critical factor will be who can make the better consensus decisions in the shortest amount of time. In short, which senior military/political body can work their Observe –Orient-Decide-Act (OODA) loop faster.

Economy of Force. "Employ all combat power available in the most effective way possible; allocate minimum essential combat power to secondary effort.[109] Optimum economy of force requires total situation awareness if finite combat power is to be employed in a timely, decisive manner. US force structure is becoming increasingly dependent on information exploitation so that it can employ just the right amount of combat power at the right place at the right time. This reliance on information can become both a vulnerability and fallible. For example in Operation Allied Force over Kosovo it was reported that NATO dropped over 3,000 precision guided weapons that resulted in 500 hits on decoys, but destroyed only 50 Yugoslav tanks. This is an important point because early in the war NATO and US stocks of precision weaponry ran very low. Economy of Force was jeopardized because of Serbian use of information denial techniques, such as camouflage, etc. Information transparency can work to either sides advantage.

In short, the US Military's Principles of War are general guidelines for how to employ force and conduct military operations. From this brief review of the principles of war it is seen transparency affects all of the principles of war to some degree – the most serious being mass, security, and surprise. In essence, proliferation of technology globally is changing the science and art of war.

Transparency - a Technology Equalizer

Besides the long established, guiding principles for war, the US has two other historical preferences for waging war. The US has been a strong technology proponent, arguing that technology is a force multiplier against numerically superior forces. The US has fought nearly all of its wars in the 20th century as a coalition member. The following sections will look at what impact transparency has on these US warfare preferences.

A tremendous faith in technology is an abiding American characteristic. The idea that superior technology can be leveraged to make up for shortfalls in numbers – be these numbers of troops, weapons, or dollars – is as appealing as it is traditional.[110] Since the beginning of the Cold War, the US has a history of relying on technology advances to provide superior firepower against numerically larger enemy forces. The US won the Cold War against the Soviet Union by buying quality over quantity. If the Soviet Union had more soldiers and tanks, the US had better soldiers and better tanks. The US has become so culturally technologically biased, that a term "force multiplier" has been coined to describe "bringing the right force to bear in the right place at the right time." The US military uses its superior technology as an asymmetrical tool for conducting warfare.

In the Gulf War, the US exploited all of its available technology to achieve military dominance. In terms of operational impact, the salient capabilities were: laser guided bombs used in combination with night-capable target acquisition and tracking devices; sophisticated night-capable tank fire control systems; the ability to operate at night; the long range precision strike cruise missiles, the widespread use of secure voice communications and facsimile machines for command, control and coordination; the advent of beyond-visual-range air-to-air combat as an operational reality; and the operational debut of airborne radar systems like Joint Surveillance Target and Reconnaissance System (JSTARS), capable of monitoring the land battle in detail.[111] Another force multiplier for US forces in the Gulf War was information exploitation.[112] National surveillance and reconnaissance, missile launch warning, navigation and leased commercial communications assets were all used to ensure successful coalition operations. More recently in Bosnia and Kosovo operations, the US has exploited technology advantages in GPS, precision target acquisition and track systems, and miniature missile navigation and guidance systems to achieve standoff, surgical strikes. The fact that these technologies were deployed against inferior adversaries does not detract from their success. Unfortunately their success was equally offset with unanticipated difficulties. Difficulties arose in applying our intelligence systems and analytical methods, controlling the swift operational tempo of the war, and achieving effectiveness given the asymmetrical response by the adversary.

Numerous papers have been written in recent years on how the coming of the Information Age will impact warfare. Alvin and Heidi Toffler argue that in the future controlling information will be synonymous with power. To them, "the value of the third wave increasingly lies in their capacity for acquiring, generating, distributing and applying knowledge strategically."[113] To a realistic military person, it means the DOD has become culturally biased towards technology over the last 50 years and automatically assumes it will continue to have the qualitative technology force-multiplier advantage. But because of the increasing rate and scope of diffusion discussed in Chapter 2, this is not necessarily a good assumption. Many others are starting to share in this force multiplier technology. Therefore in a sense, the US military needs to go back to basics. It needs to remember that its not the science (i.e., a historical US skill) or the technology (i.e., a historical Japanese skill) that makes a difference, but the time to *integrate technology into society/military and adapt the culture to it.* In this sense, the US military needs to reinvent itself to cope with the fundamental transformation occurring in war and warfare. Future wars will be won not by who has the newest technology – but by who best integrates the new technology with the right doctrine into a cohesive fighting force. The key is rapid adaptation.

Impact on Coalition Warfare

The US has fought most 20th Century modern wars as a member of a coalition.[114] Since the end of the Cold War, coalitions have been an increasing factor in dealing with collective threats. The 1999 US National Security Strategy of Engagement speaks to the US commitment to remain engaged overseas and work with allies to create international structures strengthening security and prosperity.[115] The underlying National Military Strategy asserts the US will fight future wars as part of a coalition or alliance.[116] One of the most famous recent coalition operations was the allied effort in the Gulf War. This coalition effort was, as all coalition efforts are, a transitory event, which emerged in response to a specific threat. It dissolved once the coalition goals had been met. One of the most noteworthy alliances that the US participates in is the long-standing North Atlantic Treaty Organization (NATO), created in 1949. Operation Allied Force is considered a key NATO success. Aircraft from 14 nations, operating from 47 bases, conducted a successful air campaign for 78 days over Yugoslavia, losing only two aircraft to enemy fire.

Coalition (or alliance) warfare adds another element of friction to the already unpredictable and chaotic events of war. Over the last fifty years in NATO, the US has sought to minimize the chaos by mandating standardized equipment and interoperability. But senior military officials said the Kosovo operation highlighted problem areas. One of the problem areas is in maintaining an Euro-Atlantic interoperability baseline. During Operation Allied Force, significant generational differences in equipment (e.g., incompatible European 1st generation versus US 3rd generation secure radio links) created interoperability difficulties. They also created problems in exercising effective command, control and communications (since there were three generations of technology in the field).[117] The widening gap between the US and NATO countries is causing considerable unease on both sides of the Atlantic. The coalition of the willing could potentially become the coalition of the interoperable.

Coalition fighting will only become more difficult as the technology gap with our friends widens while the technology gap with our potential adversaries closes. As NATO Secretary-General George Robertson said, "Today technology is moving so fast that some of NATO's members are in danger of being left behind."[118] Unfortunately, Allied members have not and are not making the investments in their military defense structure to keep up with US advances. European nations as a whole spend less than half of that of the US on procurement and a third of its research-and-development budget on defense. Specifically, the US spent $252.4 billion last year, in 1997 dollars, compared to $140.4 billion spent by the 16 members of European members of NATO *combined.*[119] Furthermore, European and US critics alike contend that the money European governments do devote to the military is not well spent.[120] This capability gap is expected to widen – particularly as the US military pursues Joint Vision 2010 and increases its reliance on information systems for joint operations. Therefore because of the risk that transparency may level capabilities with adversaries but widening the gap with traditional allies, the Atlantic-Euro partnership must create a new concept of coalition operations. Maintaining a stance of integrated coalition operations maybe politically correct, but it could become militarily unexecutable.

Transparency may also exacerbate tensions in Coalition politics and military execution. It may even change our relationship with our allies. Transparency requires (and causes) fast, focused decision making, but coalitions lead to slow, broad-based decision processes. During Operation Allied Force, Secretary of Defense William S. Cohen learned first hand the impact that transparency has on coalition campaign strategy, operations tempo, and tactics. He remarked, "it became clear quite quickly that NATO needed to retool its existing political machinery to be more effective for what I would call the staccato timing of a military contingency."[121] The coalition was slow to organize and commence action.[122] Furthermore, 19 countries wanted some say in or at least some oversight role in how military operations would be conducted. Political leaders became deeply involved in the day-to-day nitty-gritty of targeting decisions and casualty estimates. Individual European countries could veto both the kinds of targets that could be attacked and the individual missions. For example, press reports indicate that France's President Chirac was not fully aware of the scale of NATO attacks until he saw the television coverage of their effects on April 3, 1999. He then immediately called President Clinton and requested the ability to review all targets, including strikes in Montenegro.[123] He got his wish, but the targeting decision cycle slowed down greatly.

The overall trend is clear: NATO countries want a equal say on the major decisions in global crisis without having to possess or wield anything like equal military power.[124] They want to increase their own prestige, and make short term economic gains by taking advantage of the continuing US focus on long-term support of the international order.

For the foreseeable future, the US will remain reluctant to intervene unilaterally in most crises. The US wants others to pay for, participate with, and permit US/coalition military action. Therefore the preference for coalition partners will shape American strategy. [125] In conflicts demanding greater allied contributions, their capabilities (or lack thereof) could matter significantly. While US forces on their own may be greatly superior to an adversary's forces, if allied and partner forces have not improved their military capability to better exploit information systems, coalition operations will be more difficult and may jeopardize superiority. It may even mean that the US would have to forego using some of its advanced systems in order to facilitate combined operations. But this leaves the US in a "catch-22" situation.

Globalization, military competitiveness, and transparency mean that everyone – including our potential adversaries - have relatively rapid access to evolving technologies. The US must therefore continue to advance its military capability to protect US interests. Since the US cannot underwrite the modernization costs of our European alliance or coalition forces, it finds itself at a defining point of what coalition and alliance warfare means in the 21st century. Perhaps the US National Security Strategy should redefine the guidelines so that not all alliance partners have to fight alongside the US, only those who are willing or interoperable?[126] Either way, things must change. The enemy will not be sitting still while the US struggles to shape its alliances or coalitions into cohesive efficient military tools of policy.

Chapter Summary

Information knowledge and processing has always been part of warfare. From Alexander the Great to the present, information knowledge has played an important role in determining the outcome. But it was the Gulf War that unambiguously demonstrated the value of coalition operations and achieving information dominance in military operations. The US Military is rapidly incorporating information exploitation systems into its war-fighting arsenal. But coalition partners may not be able to keep the pace. Future partners may not adequately close the gap in technical electronic equipment generation incompatibility, language difficulties, and cultural perspectives. Political and military leaders alike will have to balance political agendas against transparency adeptness and military skills. Furthermore, the dual use technology is diffusing rapidly. A determined regional adversary could easily exploit these technologies, which the US has paid dearly for, to create their own regional sphere of influence. In future conflicts, information will be central to the outcome of battles and engagements. The winner will be the side that has the most robust, adaptable system that can meld the new technologies with innovative doctrine and adaptive organizations. The US must begin developing counters to the evolving world of transparency if it is to maintain its military supremacy.

Notes

[80] Joint Publication 1

[81] Barwinczak, Patricia M. "Achieving Information Superiority," *Military Review*, Sep-Nov 98, Vol. 78, Issue 5, p. 36.

[82] Air Force Doctrine Document 2, *Organization and Employment of Aerospace Power*, Spring 99 revision, version 5, pp. 11. (574 blue book)

Notes

[83] *The Annual Report on The Army After Next Project to the Chief of Staff of the Army,* July 1997, p. 14.

[84] *Air Force Manual 1-1*, Chapter 2, p. 13.

[85] Ibid, p. 17.

[86] Record, Jeffery, *Ready for What and Modernizing Against Whom?* Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, April 1995, p.7.

[87] Tilford, Earl H., *The Revolution in Military Affairs: Prospects and Cautions*, Strategic Studies Institute, US Army War College, 23 June 1995, p. 15.

[88] Ibid, p. 15.

[89]*Air Force Manual 1-1,* Chapter 2, p. 16.

[90] Chandler, Robert W., *The New Faces of War*, p. 231.

[91] Ibid, p. 242.

[92] Infield, Glen B., *Disaster at Bari*. New York: Macmillan, 1971.

[93] Rolfsen, Bruce, "Report: Bases near Combat Zones may be Threatened", *Air Force Times*, November 29, p. 20.

[94] *Air Force Manual 1-1*, Chapter 2, p. 20.

[95] *Field Manual 100-5, Operations*, May 1986, p. 7-1.

[96] *Air Force Manual 1-1*, Chapter 2, p. 17.

[97] Estes, Howard (Retired Gen, USSPACECOM), Testimony 1998. www.spacecom.af.mil/usspace/testim98.htm

[98] GWAPS, p. 248

[99] *Air Force Manual 1-1*, Chapter 2, p. 18.

[100] Dateline, 11/15/97, "War and Pizza," http://ur.../aa111597.htm?rnk=rl&terms= pizza+deliveries+to+the+Pentagon&PM=112 300_

[101] As quoted in Dr Andrew F. Krepinevich, Jr., Testimony Before the Airland Subcommittee, Senate Armed Services Committee on the Future of Tactical Aviation (Washington, D.C.: Center for Strategic and Budgetary Assessments, March 5, 1997), p. 4. (Chandler, pp11)

[102] *South China Morning Post*, "Spy Satellites said to Track US Warships", Oct 6, 1999.

[103] Ibid.

[104] Opall, Barbara, "China Sinks US in Simulated War," *Defense News*, February 5, 1995, p. 1

[105] Friedman, George and Meredith, *The Future of War*, Crown Publishers Inc., New York, p. 303.

[106] Air Force Research Laboratory engineers and technicians, working in what is now the new aggressor squadron's Space Electronic Warfare Flight, demonstrated how easily it is to build a mobile ultra-high frequency noise source capable of disrupting satellite links. They purchased a Honda electronic generator, copper tubing, PVC pipe from a local home-supply store and electronic components at a swap meet. They assembled these into a noise source, wrote a bit of software code to control it, mounted the system on a pickup truck and "had a working jammer." Total cost was $7,500. Aviation Week and Space, Vol 152, No. 14, April 3, 2000, p. 53.

[107] Ibid.

Notes

[108] *Air Force Manual 1-1*, Chapter 2, p. 12.

[109] *Air Force Manual 1-1*, Chapter 2, p. 18.

[110] Roland, Alex, *The Technological Fix: Weapons and the Cost of War*, Strategic Studies Institute, US Army War College, 6 June 1995, p. iii.

[111] Howard, Sir Michael, *How Much Can Technology Change Warfare?* Strategic Studies Institute, US Army War College, 20 July 1994, p. 28.

[112] Powell, Colin. "Information-Age Warriors", *Byte*, July 1992, pp. 370.

[113] Toffler, Alvin and Heidi, *War and Anti-War*, New York: Warner Books, 1993, p. 67.

[114] Silkett, Wayne A., "Alliance and Coalition Warfare," *Parameters,* Vol. 23, Summer 93, p. 74.

[115] *National Security Strategy of the US, 1999*, p. 2

[116] Hammond, Grant T., "Myths of the Gulf War: Some "Lessons" Not to Learn", *Airpower Journal*, Vol XII, No., 3, Fall 1998, p. 18.

[117] Ibid.

[118] Garamone, Jim, "Robertson Calls for NATO to do More," http://www. defenselink.mil/news/Feb2000/n02082000_20002081.html

[119] Sands, David R., "Bid to Create EU Army Stalled," *The Washington Times*, January 9, 2000, p. C11.

[120] There are 750 defense contractors in Europe compared to less than 250 in the US. Research and development funding in the US is doled out more effectively to a smaller, more efficient group of contractors. Ibid.

[121] Secretary of Defense Cohen's speech to the International Institute of Strategic Studies at San Diego, California, 9 Sept 1999, as reported in www.defenselink. mil/speeches/1999.

[122] Mann, Paul, "Fathoming A Strategic World of "No Bear, But Many Snakes," *Aviation Week and Space Technology*, December 6, 1999, p. 61.

[123] Priest, Dana., ."France Acted as Group_Skeptic, *Washington Post,* September 20-1999, pp. A-1, A-10. See also, http://ebird.dtic.mil/Sep1999/e19990920bombing.htm

[124] Kagan, Robert, "The Benevolent Empire," Foreign Policy Vol 111, Summer 1998, pp. 30. See also DFI reader p. 83.

[125] Scales, Robert H Jr., "Trust, not Technology, Sustains Coalitions," *Parameters*, Winter 98/99, Vol. 28, Issue 4, p. 4.

[126] Kosovo War Still Rages in Brussels, *Defense Week*, February 7, 2000, pp. 1

Chapter 4

Implications to US Military Competitiveness

Sometimes, looking straight ahead – even with the most dedicated attention and seasoned experience – just misses both the big picture and the new ideas, because they often come at you from "left field." Ironically, the more successful that you are, the more likely that you'll miss those seeming orthogonal ideas. Success can be your worst enemy.

Nicholas Negroponte
Cambridge Massachusetts

How will transparency impact the nature and objectives of warfare? During the Gulf War, the US amazed other countries with its ability to exploit information. It provided an unequivocal demonstration of the value of achieving information dominance in military operations. Critical information linkages between electronic warfare, intelligence, surveillance and target acquisition plus the firing of precision guided munitions from many different air, land and sea platforms simultaneously, confirmed the US belief that "what can be seen can be hit and what can be hit can be killed."[127] But this requires the seamless integration of information – information that has become both a US core requirement and vulnerability that adversaries can exploit in future conflicts.

The increasingly transparent world the US faces in the near-term has consequences. Many military analysts argue this period, 1995-2010, is analogous to the military technology evolution that existed from 1920-1935, the period between World War I and World War II. During this period, advances in the internal combustion engine, strategic aircraft capability, radio, and radar reintroduced strategic and operational mobility, maneuver, and initiative to the battlefield. The airplanes, tanks, and radios, adapted to military use in 1918, represented quantum leaps in capability over 1914. Yet the combat power represented by these same systems in 1940 was orders of magnitude greater than it had been in 1918. This major improvement in using technology was realized after only two decades of technical improvement, doctrinal development and organizational adaptation. Germany's stunning land warfare victories over the French, British, Dutch and Belgium armies in May-June 1940 transformed land warfare. Their blitzkrieg tactics achieved battlefield surprise by combining advances in tanks (including tank radios) with better organizational tactics, techniques and procedures. These changes in combined arms formations and supporting air arm opened the way for new operational concepts such as deep penetration on narrow fronts and air superiority with mission-oriented tactics. Some analysts argue that today's diffusion of advanced long-range precision strike systems, combined with information fusion and integration of reconnaissance/strike systems, with supporting doctrinal and organizational changes motivated by the Gulf War, could be equivalent in today's context to the 1920-1935 transformation. The critical turning point will be for those who better and more rapidly harness evolving technology with doctrine advancements and organization adaptation to create a revolution in military capabilities. Therefore proactively evaluating the affects of technology and information transparency is critical to maintaining US competitiveness.

An answer increasingly advocated by US military for continued information dominance is space warfare. But in the near to mid-term, using space weapons to deny an adversary's use of space will not be the answer. There are several reasons. The Army set up a war game last year, in which the US fought a fictitious Middle Eastern country, called the "New Islamic Republic." In the exercise, China provided satellite imagery of US troop movements to the enemy. That left US decision-makers debating whether to try to knock out China's satellites – which almost certainly would have drawn China into the war. Another complication was that the "New Islamic Republic" sent military communications over the same international satellites used by journalists to send their war stories back home. Should the US attack those satellites? In the end, Richard Armitage, a former top Pentagon Official who played the role of the Commander in Chief, concluded the best course of action was "to do nothing. It just wasn't worth pissing off the whole world."[128] Furthermore, while space weapons appear inevitable, Robert Bell, President's Clinton's former special Assistant for Arms Control, argues it must be a significantly compelling argument to persuade the President to cross the line. In the end, it may take a Pearl Harbor-like attack on a US licensed satellite to justify such a momentous move.[129] Therefore, space attack to deny or degrade transparency in the next 10-15 years is not wise. The US military needs to develop alternative means to cope with the effects of transparency without an over reliance on space weapons.

Considering advancements in the past ten years in information technology, what will be the advancements in the next 15 years? To what degree will transparency change the nature and objective of future war? The US needs to keep a sharp eye out or it will find itself in a situation similar to 1940, when a regional power, Japan, became more than a match for the US Pacific forces during the early phases of World War II. The US military must therefore position itself now to adapt to the evolving transparency caused by technology diffusion if it is to remain a military superpower.

More will be required than just sophisticated technology. Deliberate innovation in organization and doctrine must be initiated to mitigate the openings that information transparency provides to a potential adversary. Forces that are well trained, well motivated, and well led will be needed. Their operations will greatly depend on an effective doctrine.

Innovate Doctrine

The accomplishments of the US military in the Gulf War and its continued incorporation of information technologies into the mainstream military has led to a significant asymmetrical advantage over the rest of the world. But rather than continuing to gloat publicly over these advantages, US military strategists must give hard thought to the limitations of the new evolving weapon systems. Assessments must be made of the second and third order effects on the doctrine for employing the new weapons systems and align that doctrine with America's true politico-strategic aims and interests. While several potential modifications are proposed below, the list is by no means complete.

Rethink Joint Vision 2010 Strategy. Joint Vision 2010 was published by the Joint Chiefs of Staff to create a broad framework for understanding joint warfare in the future and to direct the service's acquisition programs towards acquiring the capabilities to achieve four types of operations: precision engagement, dominant maneuver, focused logistics and full dimensional protection of forces and assets. A key tenet of the strategy is to exploit information systems and satellite sensor systems to achieve information dominance for dominant battlefield maneuver. This information dominance allows US commanders to detect enemy forces, maneuver and fire with greater effectiveness, while using combat power and logistics support with greater efficiency.[130] Unfortunately, the global marketplace is rapidly diffusing information technology advances to other countries. They too will be able to pursue qualitative improvements – but at relatively modest cost – to more effectively operate on the battlefield. Therefore, the US Joint Vision 2010 is at risk because of this increasing mutual transparency. Information superiority is becoming a perishable commodity. In future conflicts, the winner will not be who has the better information technology – but who has a more effective strategy that the opponent can not match or counter.

One way the US can maintain a more effective strategy is to speed up its decision making. This is essentially upgrading John Boyd's "Observe-Orient-Decision-Act (OODA) loop into what Dr Grant Hammond calls the "OODA point."[131] Technology and doctrine should be deliberately melded together to change the time-space dimension of warfare into a non-linear parallel (or simultaneous) form of war where connectivity is more important than distance. The simultaneity of employing overwhelming combat power throughout the breadth and depth of an operational area requires our information exploitation systems and connectivity to be better than an adversary's. As it also requires a new mindset away from linear battlefields and controlled decision making. The US military should strategize and practice how this non-linearity would work, train for reduced decision making time, and modify weapon system equipment acquisitions for extreme modularity to best exploit this rapidly evolving transparent global world. After all, as per Moore's law, every eighteen months processing power doubles while costs hold constant.[132] By 2010, air, naval, and ground operations will operate at faster rates over longer distances. Combat could either resemble a fast break in basketball (the goals of WWI combatants) or a running game in football (the realities of WWI).[133] Since everyone will have access to much of the same basic technologies, the key will be in who has the better strategy and can better adapt to the changing, unknown and unknowable, future world contingencies. Since it is physically and financially impossible to prepare for all contingencies, the focus must shift to a rapid adaptive capacity capable of dealing with the most probable contingencies. Lastly, Joint Vision 2010 with its emphasis on high technology solutions to future conflict is silent on how to re-fight a counter insurgency like Vietnam or any future small-scale contingency where diplomatic coercion is the chosen policy. Therefore, it would be well advised for the US military (particularly in light of Kosovo, Bosnia, and Somalia) to expand its doctrine.

<u>Devise an Escalation Doctrine</u>. "The political objective is the goal, war is the means of reaching it, and the means can never be considered in isolation from their purpose."[134] This Clausewitzian expression is as true today as it was back in the 1800s. With the increasing need to contain small-scale conflicts, the US military must develop effective joint strategies and doctrines to fulfill the NCA's need for escalation compliance or coercion (vice overwhelming parallel warfare). Given the US military's experiences in Kosovo, today's "hot spot" global climate, and the lessons of Vietnam, it seems realistic for US military to add this capability to their arsenal. This is needed before an adversary creates an asymmetric spin that drives the US and its partners into another "tit-for-tat" escalation mode.

The recent NATO conducted Operation Allied Force in Kosovo underscores the need for a new "less than total war" mentality. As the NATO's Supreme Allied Commander, Europe, General Wes Clark believed the only way to prosecute the Kosovo war was to go for the first-round knockout by hitting the Serb troops hard right from the start. He wanted to avoid the quagmire of Vietnam where the military was too cautious and the politicians too restrictive. Unfortunately while General Clark believed that we should win 21 to nothing there were some who preferred to win by a score of 7-6.[135] Apparently, the overwhelming force attacks in the middle of the night were viewed as excessive force that did little except level the infrastructure of Yugoslavia. Late last July, just after the conclusion of combat operations in Kosovo, General Clark was notified of his retirement.[136]

Essentially General Clark was sort of a lightning rod for criticism of the policies of engagement in the Balkans. Since the end of the campaign he has been reassessing his decisions. In November 1999, he stunned the US Senate Armed Services Committee when he called for a complete rethink of Western Strategy and questioned the need for the aerial assault on Serbia. General Clark noted that NATO could have used legal means to block the Danube and the Adriatic ports, and could have used "methods to isolate Milosevic and his political parties *electronically*."[137] If implemented and augmented with other measures, Clark added; *the military instrument might have never been used.*[138] Others in NATO concur.

At the recent NATO conference in Brussels on Kosovo, Sir Michael Alexander, chairman of the Royal United Services Institute for Defense Studies in London, argued for the development of an escalation strategy. "Anyone who believes multinational coalitions or gradual escalation won't be a part of NATO's future is fooling themselves. In democracies," he said, "gradual escalation is the name of the game, because the only circumstances in which our governments could talk of the ground force option is when the horrors of the ground really began to impact on public opinion to the extent that the politicians felt they could get away with it. That is going to be the case in the future."[139]

Rethink Coalition Operations. Operation Allied Force demonstrated, on both sides of Atlantic, the dismal status of timely coalition decision making and interoperability. Over the last ten years, generational equipment incompatibility has arisen between the Armed Forces of the US and those of its allies. European forces can only be interoperable and effective military coalition partners if they acquire capabilities similar to those of the US or tailor their forces to use US systems. Unfortunately, although in NATO committee meetings and to the media, they "talk the talk," when it comes to appropriating the various national budgets, defense spending remains low.[140] Furthermore, the European position is obviously for the US to license co-production to European Defense contractors.[141] This is unlikely to happen, as there is no compelling reason for an already constricting US defense base to give up its business and trade secrets.

The US must apply its scientific and technical strengths to develop a multi-level security open system architecture that allows coalition partners to connect into the US based C4ISR system. This way, the US can maintain its revolution in military affairs plus establish downward compatibility with established alliances and future coalition partners. Allied defense contractors could participate in the creation of the standard – but with the understanding the US will continue to push its information revolution with faster processing speeds, data rates, data fusion techniques, organizational adaptations, and revised military doctrine. It would not be held back in developing future capability to counter unspecified future threats to its national defense.

Coalition consensus decision-making is too slow. In the age of transparency, this is unacceptable. Therefore the US must help NATO learn to react within the enemies decision loop. The US must lead NATO in developing a new command and control structure that maintains coalition unity but reacts in a more timely manner. The DOD must consider various methods to speed up or focus the coalition decision process - even at the risk of some loss in security.

Integrate Camouflage, Concealment & Deception both vertically and horizontally into Military Operations. "The history of warfare suggests that there are always countermeasures and human ingenuity will finds its ways to confuse the enemy," said Eliot Cohen, a professor at Johns Hopkins.[142] From the use of the Trojan horse to Serbian mockups that look like tanks, deception has been used to stymie a more powerful army. The US used mockups of tanks and landing craft leading up to D-Day to fool German aerial reconnaissance into believing the attack to be at Calais, instead of at Normandy. The DOD should go back to basics and actively incorporate deception into all organizational levels and all levels of warfare. Chinese and Russian strategists alike routinely practice measures such as camouflage, deception, dispersal, mobility and secrecy to limit an adversary's information. In fact, the Russians taught the Iraqis and Serbians. The US needs to take area seriously and incorporate the techniques all the way from the strategic level down to the squadron, company, and platoon level.

Furthermore, the Serbs shot down the Air Force F-117 stealth fighter by using spies to monitor the plane's takeoff from Italy and then low tech, long shot tactics to shoot it down. Despite common sense knowledge, the US military has a history of waiting for incontrovertible proof (i.e., military setback) to alter tactics or vary operational parameters for such routine things as departure times. Why is it the US military keeps learning this lesson over and over again? Its hard to believe that in today's mission planning cells, with its powerful computers, the US can not increase agility into its operations!

Conduct Commercial Technology Symposiums to Maintain Robust Doctrine. Lastly, since technology is a key input into doctrinal evolution, the DOD must make a concerted effort to host commercial (not defense based) technology symposiums or tour commercial facilities. The technology that the military is exploiting today has come to depend heavily on the commercial world. The US needs to do a better job of capturing that commercial knowledge base if it is to maintain a vibrant doctrine. The service laboratories are not the designated eyes and ears for the doctrine centers. The military can periodically tour commercial technology centers and get that information in front of as many people as possible to evaluate.[143] In short, the US needs to develop the processes to experiment or wargame with newer doctrinal concepts. Without such efforts, the military faces the risk of becoming increasingly insulated from the real world and real capabilities.

In the years ahead, the US will need not only a flexible and adaptive force posture with sufficiently large and diverse assets, but also an effective doctrine and planning framework for guiding force preparation. When is the last time the US seriously modified it? There are multiple threats with multiple agendas. How fast can it respond to these dynamic changes in the "business sector" called war?

Selected Technology Development to Counter Transparency Effects

Technology is constantly advancing – particularly in a world that is organized to conduct scientific research and engineering research on a large scale. The armed forces of a country, such as the United States, that depends heavily on technology must constantly innovate in order to stay ahead. In addition, as has been underscored by the tragic US experiences in Somalia in 1993, inconclusive aerial attacks against Iraq in 1998, the human cost for Kosovar Albanians in the NATO war against Serbia in 1999, the vulnerabilities of modern societies to missile and terrorist attacks, our technological edge has its limitations even today.[144]

US adversaries, even if considerably less technologically sophisticated and wealthy than the US, can benefit from the global economy and increasing transparent world. They can acquire and learn to make good use of precision missiles, satellites, advanced mines, weapons of mass destruction, and computer viruses and thus be able to challenge US operations much like the Serbians did in Operation Allied Force. As a result, the US needs to seek new military concepts to overcome these challenges to its military supremacy. The following technological based ideas are submitted for consideration.

Reinvigorate the Science of Data Analysis and Interpretation. The Chairman of the Joint Chiefs of Staff, General Henry H. Shelton, recently noted that "information operations and information superiority are at the core of military innovation and our vision for the future of joint warfare. The capability to penetrate, manipulate, and deny an adversary's battlespace awareness is of utmost importance."[145] Kosovo, unfortunately, exposed problems with this concept. In spite of NATO's near total information superiority, its battlespace awareness was manipulated by the Serbian armed forces more often than expected. For example, strikes on fake targets indicate that the Serbs let NATO daytime reconnaissance flights see real targets then replaced them at night, or that US target analysts misinterpreted the (digital) information furnished them. They essentially developed low-tech offsets that limited the effectiveness of NATO's information superiority and misled NATO collection assets. In other words, they succeeded in misleading US information interpreters.

When the human and software interpreters of intelligence were fooled, it resulted in munitions wasted on fake or incorrect targets and in bad assessments of the actual situation on the ground. Hitting the right target on time requires sorting out the right coordinates from a pile of information (interpreted correctly) at the right time. This requires a degree of data management that is difficult to achieve. Therefore it is time to challenge the scientific community to see if they can help the digital interpreters quickly and correctly sort through and interpret the cascading amounts of information, that confront them. to find the "one needle in the haystack" that will pinpoint a target in the right time frame. Techniques that could be considered include such things as improvements in battlefield visualization, language translation and cultural identifiers, automated comparison to non-technical possible asymmetric techniques, analysis of the methods and sources used or study non-technical offsets used to interpret data.[146] Until we can get improve the analysis of the overwhelming inflow if data, intelligence and targeting analysis will continue to be the weak link.

Develop Faster Decision-Making Processes. Because the side that wins in future conflicts is the side that better adapts to the changing environment, the US must exploit its advantages in information processing through much faster decision making. During

Operational Allied Force NATO did not process information quickly enough to enable aircraft to strike mobile targets. This was because of the reaction time required to pass data from EC-130 (airborne command, control and communications) aircraft to NATO's Combined Air Operations Center in Vicenza, Italy, and then on to strike assets.[147] It is now time to deliberately improve the process. We must refine the "observe, orient, decide, act, or "OODA loop," into an OODA point." The intelligence collection and dissemination system must be more real-time, include information validation, be able to work their way through dense waves of data, and in today's world, and provide useful predictive analysis on intentions. As Mr. Keith Hall testified to the Senate Armed Forces Services Committee this spring following regarding Kosovo, "We have to find ways to collapse that cycle of collection management tasking, collection processing exploitation, and dissemination, and move it from what has been past, days, or at least hours, to minutes."[148] Furthermore, decision-makers must be trained at all levels in OODA point decision making. Future commanders will have to be trained to use the information systems and their knowledge/intuition so that they can make those risky decisions rapidly and continuously. This training must include US alliance partners as well. They must also be supported by systems able to process more and more information with less and less time.

To support OODA point decision making requires Intelligence analysts to have the best state of the art commercial imagery equipment, multi-media indexing technology, and real-time distribution systems so that – assuredly - the right information gets to the right person on the first try. This is easy to say but a lot more difficult to do. Furthermore, for the foreseeable future, the US is likely to be engaged in relatively small-scale regional conflicts where leadership, cultural symbols and political motivation are critical key factors. Furthermore, since many intelligence reports are often contradictory, we must develop methodologies and processes to cull out the valid information in near real time. We must develop or exploit commercial database mining techniques, appropriate to our adversary's culture, to order to get the right information on such things as intentions and indications.

We must also do better at exploiting unmanned air vehicles (UAVs).[149] UAVs provide an important surveillance and reconnaissance capability. They can gather targeting and intelligence data at low altitudes, under poor weather conditions, and at night and feed the targeting and reconnaissance system with information that space-based and higher altitude sensor systems cannot gather or cannot provide with sufficient real-time flexibility and resolution. Unless we can do "the observe and orient phases" of the OODA process with validated information, we will end up with misinformed decisions and inappropriate actions.

Lastly, we must create flexibility in our "act" phase so that we can be immediately responsive to the unfolding situation. The creation of a "dynamic ATO process" would allow command centers from the rear to update targeting information while strikes are still in flight, or to alter their missions, to reflect new data on the overall course of the campaign and threat air defenses.[150] This can be accomplished by directly linking mission planning and air control systems to the strike aircraft so they can change in real-time the mission of strike aircraft, regardless of the number of allied aircraft in the theater of operations. In theory, this can be done immediate by automating procedures – such as were used in Vietnam for in-country air support. The doctrine exists – it's now time to automate and standardize. In short, the technology is there for the harnessing – its time for the organization to experiment with it under crisis conditions. Unless we can improve each element of the OODA loop, we will never improve our overall OODA process into a fast reacting, dynamic OODA point.

Improve Sensors: Deny Utility of Deception. The US is increasing its reliance on remote sensors to pinpoint and long-distance weapons to strike tactical targets. We then destroy the target by launching general-purpose shoot-to-coordinate weapons at it. Because most fielded US sensors can't see inside things or distinguish between a decoy covered in metallic foil and the real thing[151], the likelihood exists that our commanders will not have sufficient confidence in targeting elements and information to act decisively. In the recent Kosovo conflict, Serbia used wood and plastic sheeting, metal tape, and metal plates to build phony targets of mockup tanks, armored personnel carriers and other ground decoys. The US therefore needs to aggressively develop the technology and methodology for weapon systems to detect concealed, mobile targets and distinguish the real targets from mockups. Such considerations may include image fusion of infrared, panchromatic and other sensors geo-spatially registered so that they can verify a target is really what it is supposed to be and speedily forward that information to the pilots firing missiles or dropping bombs. Cross sensor real-time data fusion is a possibility and potential requirement for knowledge validation. In the Kosovo example above, the radar alone would be confused, but infrared, which sensed surface temperature, could detect if an engine had recently been used, and signal intelligence could see if normal communication patterns were occurring among the tanks.[152] All of this would make decoying more difficult.

Develop a Fiber Breaking Weapon. If the US is serious about degrading the enemy's command and control infrastructure, it had better start upgrading its munitions. Advanced wide-band cable transmission technology continues to proliferate at an accelerating rate as more countries and companies deploy Internet transmission infrastructure. The company, Global Crossing, states that by the end of 2000, their network will include access to 80% of the world's major traffic routes.[153] They face stiff competition from other relative new companies like Project Oxygen to provide any customer with high speed, high connectivity fiber optic routing worldwide.

Yet as mentioned earlier, these fiber optic based advanced networks are particularly tough to put out of action with precision guided munitions.[154] In the Gulf War against Iraq[155] and again during Operation Allied Force, [156] in the Balkans in 1999 against Serbia, there were serious problems in attacking the command, control and communications systems. Both Iraq and Serbia had made extensive use of commercial telephone switching networks and multiple buried fiber optic cables. These facilities are militarily difficult to degrade yet quickly repaired with redundant connectivity. (While a precision guided munitions strike against below ground junction stations could completely destroy the aboveground structures, the fiber optic line often remained intact unless cut later with repeated attacks with precision guided munitions.) The US military has not yet developed a way to successfully take out this new communications transmission medium. Therefore, given the proliferation of fiber optic networks and US military emphasis on degrading the enemies' capability, it is time to start addressing the next difficult problem.

Countries can very often find shortcuts in incorporating information technology and attain similar standards to those of the US's within a short period of time. Therefore the

DOD must look at ways to improve and tailor the procurement system so that it can be more responsive to the evolving threat environment. But just developing the technology won't be enough. Technology must be rapidly integrated into the military and adopted into the art of war.

Adapt the Organization

Improvements in doctrine and technology can enable US forces to remain a preeminent military power. But it can not do it alone. Joint Vision 2010 prescription for achieving information dominance is flawed because it does not adequately take into consideration the diffusion of commercially based information and communications technology and the subsequent erosion of US advantages. The winner of the next war will be who can best execute and adapt their strategy to the war at hand. In short, who has the better training? Evidence is mounting that the interaction between the technology and user methods and skills profoundly influences combat outcomes.[157] Therefore, the US must inculcate into all levels the dual use of information – information as a tool and as a weapon – for either side.

Maintain Quality Force Quality is a relative thing as much depends on the quality of the adversarial forces. But given the increasing proliferation of technology around the world, the US military must not only equip its forces with the most advanced technology, but also (equally important) continue to recruit and train high-quality personnel. This is more important than ever because poor skills create vulnerabilities in the form of mistakes that even an enemy with lesser technology can exploit. Furthermore, with poor skill levels it will be impossible to conduct sophisticated tactics and operational routines to get the most out of the new systems coming on line.

As it is now, maintaining a highly skilled quality force is a difficult thing to do today. With the volunteer force influenced by a host of factors such as a robust economy, tight civilian labor pool, high operational tempo, and potential for casualties maintaining a quality force is difficult. But we must not back away from recruiting a quality force and providing sufficient training throughout service member's careers to insure we have the needed skills and expertise. Moreover, a much more robust retention program with selective bonuses or professional pay for people other than the type for pilots and doctors is required. Keeping computer programmers, photo analysts, and other transparency negating skills is essential for today's military and so must be incentivized accordingly. With the evolving transparent world, this becomes more and more important.

Practice Knowledge Operations. The Gulf War demonstrated unambiguously the value of achieving information dominance in military operations. The US Armed Forces used 188 mobile ground stations and twelve commercial satellite terminals to process satellite communications during the war. Linkages to US databases and networks were complex – up to 700,000 telephone calls and 152,000 messages were handled every day. In order to conduct the 42-day air war, more than 30 million telephone calls were necessary.[158] The combination of database management systems and airborne and satellite sensor system fusion permitted theater air commanders to implement the campaign strategy with appropriate mission execution. The quantity and quality of data made it possible to respond rapidly to changing circumstances. In the future, the US must not only protect our information-based systems, it must also validate information streams (to detect adversarial data manipulation), make its decision cycle shorter than the enemy decision cycle and assume the adversary will seek to radically improve his decision cycle and degrade the US. In short, the US military must inculcate into its thinking that data is a modern weapon.

To limit the US ability to exploit information sources, the enemy could kill or temporarily blind a satellite. Commandos could attack ground stations that serve as control centers or relay points for data. In the 1980s, one could take down the whole US satellite control network by taking out one building at Sunnyvale, California. The US knew of its vulnerability, but the need was never high enough in the funding priority to correct. It is time to reevaluate priorities. Furthermore, soon over 70% of US military communications will be carried commercially. Security is almost non-existent at most commercial satellite operations centers. Therefore the US must be willing to pay for "fail soft" commercial satellite communications services, create backup ground stations and implement other fixes to limit vulnerabilities. One such innovative approach could be a "CRAF-like agreement" with commercial satellite communication providers including automatic rerouting schemes prepaid in advance for emergencies. Protocols could be established which govern how military communications traffic would be switched over in time of need.

The US must also exploit information better than any adversary. The US must create a web-like C4ISR imbedded systems-of-systems that cohesively combines information into useable knowledge. Lessons drawn by senior US Air Force officers from Kosovo operations point in this direction. First is the need to develop integrated targeting and reconnaissance systems that can pass targeting data, via secure communications, on to strike aircraft in flight who can then apply the real-time data in-flight to modify missions and conduct precision strikes. But to pull this off will require *attention to the details in* *the data base and software execution process* – something military program managers tend to gloss over. A concerted effort will need to be made to re-emphasize this very difficult area with in Air Force Material Command.

Practice "Overloaded" Decision-Making. One of the most interesting and underrated lessons learned from the NATO operations over Kosovo was that "information superiority overload can actually hurt mission performance."[159] When people where beset by too much information, they lost track and do not know what to pay attention to. As Admiral James Ellis, Commander-in -Chief of NATO's Allied Forces Southern Europe, noted in an interview on Kosovo in early September 1999, "too much information has the potential to reduce a military leader's awareness of an unfolding situation. Too much data leads to sensory overload. Information saturation is additive to the 'fog of war'...uncontrolled, it will control you and your staffs and lengthen your decision-cycle times."[160] Admiral Ellis extended this problem to video teleconferencing as well, since it can become a "voracious consumer of leadership and key staff working hours." [161]

If we are to remain superior in the age of information transparency, we must become more adept and faster at information manipulation. This requires the US military deliberately establish mechanisms to teach its future leaders how to deal with information overload or information chaos. This teaching and practicing must be conducted across all levels – strategic, operational, and tactical. For the tactical level, the Army, AF, and Navy can learn from recent Marine Corps activities. The Marine Corps Gazette publishes tactical decision game scenarios monthly. The solutions are published both in the Gazette and on line two months after the problem's publication. Contributors get credit for the best-proposed solution emailed in! For other levels, Professional Military Education sponsored war game simulations and real-time computer based exercises would be very beneficial. Anything that would teach its future leaders how to make intuitive decisions under pressure with an overwhelming but incomplete data set is a step in the right direction towards successful combat engagement in the age of transparency.

Revamp Forward Basing Concepts. As mentioned earlier in Chapter 3, the Air Force needs to rethink where and how it sets up bases near combat zones to better protect its aircraft and people. The RAND report warns that an enemy armed with cheap versions of cruise missiles or ballistic missiles could devastate aircraft parked on unprotected flight lines when the bases are a few hundred miles from the battle zone.[162] Therefore, the Air Force should take actions to minimize its footprint near and around the combat theaters. Examination of distributed mini-basing concepts should be considered. The Global Engagement IV wargame supports this but does not go far enough - it ignores the impact of transparency. The After Action Report asserts that warfare in 2010 will require the US to shorten the current accepted time requirements for getting combat power to the crisis area. It recommends that forward support and forward operating locations be established regionally to enhance expeditionary force operation.[163] The individual footprint of these forward-operating locations must be minimized so that they too don't be come targets for terrorists or potential enemies. Combat operations can use a theater wide precision timing system to plan and adjust events in real time so that participating strike aircraft, originating from geographically dispersed areas, mass into the strike package over the combat area just seconds prior to attack. The aircraft can launch their advanced GPS/INS munitions to concentrate in time the precision strike damage.

To support truly expeditionary air force operations, the Air Force needs to realistically address synergistic impacts that fewer overseas and collocated operating bases and transparency has. The shrinking number of airfields in the various Area of Operations (AORs), helped create the 300+ aircraft basing problem at Aviano Air Base during Operation Allied Force. Although there are many logistics and operational considerations that drive an operation like Aviano's, limited numbers of airfields is certainly a major one. Therefore, given the evolving effects of transparency, the Air Force needs expand its numbers of airfields for expeditionary force usage. One of the ways it can do so is by changing the definition of bare basing.

The traditional bare basing requirements of water and a runway need to be updated to water and a flat surface that can support aircraft operations. The point being, in some cases an unobstructed length of dirt or highway will meet the requirement, and may be the only option available. Flying operations on dirt airstrips is currently limited to rotary, light fixed wing, and tactical aircraft, specifically the C-130s. While some dirt airstrips can be fortified with polyurethane folded mat (PFM) to minimize ruts and erosion, the limiting factor is the soil bearing capacity. Therefore, a potential dirt airstrip would have to be surveyed and soil tests completed to determine if sustained operations were possible. Climate and weather would be obvious considerations, as you can operate off frozen dirt, but not mud. Another possible consideration is use of highways with PFM (i.e., fiberglass mats) laid on top. Here, advanced surveys are necessary to find the best "contingency" airstrips; defined as those that are wide, flat stretches of roadway, that can easily be cleared of obstructions and has adjacent areas for aircraft parking and logistics operations. The survey must also determine the pavements load-bearing capability and to what degree a PFM overlay can help or minimize damage to the underlying highway. These are only thoughts to get others motivated that the effects of the evolving transparency can be mitigated through several deliberate steps.

Conduct realistic war games: Lose a few at all levels. Realistic war games and exercises, enhanced for information operations, must be conducted that either corrupt or outright jam the communications links or degrade GPS timing and navigation data. US combatant troops in the field as well as the reachback Combined Air Operations Center (CAOC) must learn now to deal with the inevitability of information corruption or denial. Where are the people charged with developing the needed new training? Who is in the back room messing with the electronic words and images? White washing away jamming, or communications delays or intelligence data overload helps no commander at any level.

In a similar manner, OSD needs to re-establish a separate "RED TEAM" organization in the acquisition community, or better yet the JCS, to independently assess the improvements being made to offset vulnerabilities. The charter which already gives JCS responsibility for interoperability testing could be used to set up the red team.. Leaving this assessment in the hands of the very organizations charged with the development is literally letting the "fox into the hen house."

Chapter Summary

So, what will we do when we are caught by an asymmetrical threat? We must develop the right future systems that can be readily adapted to fight the fight at hand. We must have a robust doctrine that can define a coercive strategy to "shape" the world. Above all we must adapt the DOD to fight the battle for information superiority in an age of transparency. Unfortunately, DOD is not set up to respond to rapid shifts in the threat environment or the increasingly transparent global market place. It needs to make deliberate shifts in doctrine, procurement and organization if it is to remain competitive in the age of global transparency. If we do not, people can and will catch up with us. Without such improvements, it is not a matter of if we will lose a future war. It is only a matter of when that will happen.

Notes

[127] Schwartzstein, p.238.

[128] Newman, The New Space Race," *US News and World Report*, November 8, 1999, p. 37.

[129] Ibid, p. 38.

[130] *Strategic Assessment 1999: Priorities for a Turbulent World*, National Defense University, p. 266.

[131] Col. John Boyd (Retired) conceived of proper strategy as one that disrupted or incapacitated the enemy's ability to cope by forcing him to operate at a tempo beyond his ability to respond effectively. Success favors the side that can observe, orient, decide, and act (OODA) sooner than the enemy. Meilinger, Col Phillip, *The Paths of Heaven: The Evolution of Airpower Theory*, Air University Press, 1997, p. 592.

[132] Downes, Larry and Chunka Mui, *Unleashing the Killer App*, Harvard Business School Press, Boston MA, 1998, p. 21.

[133] *Strategic Assessment 1999: Priorities for a Turbulent World*, National Defense University, p. 269.

[134] Clausewitz, Carl Von, *On War*, Princeton New Jersey, 1976, p. 87.

[135] Silher, Laura, "He won the war. He lost his job." *Talk*, April2000, p. 138.

[136] Ibid, p. 139.

[137] Borger, Julian, "Cyberwar Could Spare Bombs," *The Guardian*, 5 November 1999, p. 17.

[138] Ibid.

[139] "Kosovo War Still Raging in Brussels," *Defense Week*, February 7, 2000, p. 3.

[140] Both France and Germany cut their defense expenditures, including procurement, in the summer of 1999 at precisely the same time they were talking about new modernization efforts and defense cooperation. Cordsman, Anthony, "The Lessons and Non-Lessons of the Air and Missile Campaign in Kosovo, " Center for Strategic and International Studies, Revised 29 Sept 1999, p. 185.

[141] Morrocco, John, "Kosovo Reveals NATO Interoperability Woes," *Aviation Week and Space Technology*, 9 August 1999, p. 32.

[142] Schmitt, Eric, *"Bombs are Smart. People are Smarter."* New York Times, 07/04/99, Vol. 148, Issue 51573, Section 4, p. 6.

Notes

[143] Downes, Larry and Chunka Mui, *Unleashing the Killer App*, Harvard Business School Press, Boston MA, 1998, p. 124.

[144] O'Hanlon, Michael, *Technological Change and the Future of Warfare*, Brookings Institute Press, Washington D.C., 2000, p. 2.

[145] Information superiority is based on dominance in three areas: intelligence (with surveillance and reconnaissance support), C4 (command, control, communications, and computers), and information operations. US Joint Chiefs of Staff, "Information Operations," March 1999, p. 1.

[146] Thomas, Timothy L., "Kosovo and the Current Myth of Information Superiority," *Parameters*, US Army War College Quarterly, Spring 2000, p. 15. See also http://carlisle-www.army.mil/usawc/Parameters/00sprintg/thomas.htm

[147] Ibid, p. 15.

[148]Unofficial Transcript: USCINCSPACE Testimony Before the Strategic Subcommittee of the Senate Armed Services Committee, 8 March 2000. Official transcript at http://www.senate.gov/~armed services/hearings/2000/f000308.htm

[149] Cordsman, Anthony Endnote 185. *Aviation Week and Space*, August 23, 1999, p. 30.

[150] *Janes Defense Weekly*, 9 September 1999, p. 13. (Cordesman, p. 76)

[151] Friedman, George and Meredith, The Future of War: Power, Technology and World Dominance in the 21st Century, Crown Publishers, New York, p. 319.

[152] Ibid, p 320.

[153] Global Crossing, http://206.132.184.108/index.asp

[154] *Gulf War Air Power Survey*, p. 70.

[155] *Gulf War Air Power Survey Summary Report*, Department of Military Studies, Air University, Maxwell AFB, AL, p. 67.

[156] Cordesman, Anthony H., *The Lessons and Non-Lessons of the Air and Missile Campaign in Kosovo*, Center for Strategic and International Studies, Sept 29, 1999, p. 120.

[157] Biddle, Stephen and Wade P. Hinkle and Michael P. Fischerkeller, "Skill and Technology in Modern Warfare, *Joint Forces Quarterly*, Summer 1999, p. 19.si

[158] Chandler, Robert W., *The New Faces of War*, p. 337.

[159] Thomas, Timothy L., "Kosovo and the Current Myth of Information Superiority," *Parameters*, US Army War College Quarterly, Spring 2000, p. 20. See also http://carlisle-www.army.mil/usawc/Parameters/00sprintg/thomas.htm

[160] Grossman, Elaine, "US Commander in Kosovo Sees Low-Tech Threats to High-Tech Warfare," *Inside the Pentagon*, 9 September 1999, p. 1.

[161] Ibid.

[162] Rolfsen, Bruce, "Report: Bases near Combat Zones may be Threatened", *Air Force Times*, November 29, p. 20.

[163] Air Force Wargaming Institute, *Global Engagement IV After Action Report,* draft received 6 April 2000, p. iv.

Chapter 5

Conclusion

The only constant in our business is that everything is changing. We have to take advantage of change and not let it take advantage of us. We have to be ahead of the game.

Michael Dell
Dell Computer Corporation

The appearance of the written word, a few millenia before the invention of the printing press in the 17th century, transformed military power. It enabled the preparation and dissemination of complex orders and the delegation and coordination of operational and tactical command functions and organizing logistics. As a result, larger armed forces could be mobilized, logistically supported, and deployed effectively in combat. Extended operations by larger forces made command and control even more important, a trend that continued with the advent of the telegraph, telephone, and radio. Today's exponential growth in the microchip's computing power, the availability and affordability of high-speed information technologies, and global proliferation of networked public information centers enhance the ability to gather, analyze, and disseminate data and enables its manipulation via real-time movement of electronic words and images. The desire for more information to reduce the fog of war remains unabated with the advent of information technologies.[164]

Today's information revolution is analogous to the written word revolution. It is the catalyst for economic, political and military change on a global scale. Economic globalization and commercial technology diffusion is making the world more transparent, where anyone can know the business of anyone else. As the technology diffuses, so to potentially does the US military technological lead.

Despite our efforts to restrict the rate of technology transfer, commercially based information technology is rapidly and irreversibly proliferating around the world. As foreign militaries incorporate information technology and public data sources into their doctrines and tactics, transparency has the potential to seriously erode our position of dominance unless US forces plan for and use this transparency to their advantage. Chinese open source publications often discuss how the revolution in information favors a country like China more than the US. They give two reasons for this position. The first is that, because of its gratifying experience in the Gulf War, the US military has become complacent and reluctant to part from its existing military force structure and concepts. Consequentially, future enemies can use this conservatism and evolving information transparency to revolutionize their military capabilities by using more advanced thinking than the US.[165] (This is analogous to the growth in Germany's military capabilities during the inter-war period of 1920- 1938.) The second reason given by the Chinese is that the proliferation of information technology is eroding the US superiority in information dominance. To a great extent, some of the world's most advanced technology is widely available on the commercial market. Chinese strategists point out that the US overestimates its ability to gain information superiority in the face of a determined adversary who has a well-established program to deny accurate information to US sensors.[166] The diffusion of technology towards global transparency makes it more feasible to impede if not deny power projection to the US military. Clearly the Chinese feel that whoever has the better doctrine to employ the new information technology will have the key to success on the battlefield.

Proactively evaluating the effects of technology and information transparency is critical to maintaining US competitiveness. A major problem for the US has been the failure to think and talk properly about transparency's impact on future warfare and national security. "Information Warfare" jargon and its details obscure looking at the bigger issue. The bigger issue is transparency, the result of the diffusion of information technology. Transparency will impact the nature and objectives of war, just as earlier technological change did in 1920-1935.

Transparency can be expected to erode US information superiority and will have a marked impact on the principles of warfare as understood by the US military for almost 90 years. The enemy can exploit transparency to see in near real-time US actions; therefore, *mass, security, surprise, and to a lesser degree maneuver, objective*, and *offensive* are harder to achieve. Bases and seaports are now at greater risk of enemy attack. In the future there may be no choice but to disperse forces in time and space to keep them safe from enemy attack. This may in turn – with sufficient fore thought - impact the principles of unity of command, economy of force and simplicity.

Transparency will also effect how the US exploits technology to maintain its military competitiveness. Because transparency has essentially an information leveling effect, the US will have to first, seek ways to maintain its technological advantage and second, develop strategy and tactics that exploit transparency to its advantage and its ability to successfully wage war. It must investigate the possible impact of transparency on military doctrine, modernization, and organization. Several measures are proposed in this thesis. In terms of doctrine, the US needs to rethink how it is positioned to meet the goals of JV2010, rethink how it is positioned for coalition operations, and instill in its troops the notion that information is a weapon. The DOD must employ camouflage, conception, and denial (CC&D) at all levels to deny a potential adversary information. It must also improve its various sensors to see through CC&D, create weapons to destroy fiber optic networks, create decision aids for intelligence analysts and improve decision processes (i.e., OODA point) for moving target destruction. We must consider revamping our organizational structure to minimize the US military footprint near and around regional combat theaters. Lastly and possibly most importantly, we must develop and focus training on making the correct decisions while under pressure and with too much incoming inclusive data. In essence, a concerted effort needs to be spent addressing the reality of transparency and its impact on US national military strategy.

This is a compelling age in history. The exponential growth in globally marketed information systems with dual use technologies and products is creating a transparent world. But this transparency has ramifications on both how the US military will fight and how it will prepare to fight. If the US military wants to maintain its competitive position, it must evolve doctrine, acquire superior weapons and systems, and adapt a viable organizational structure. If we fail in this, commercial technology diffusion and advances will outstrip doctrinal and weapon system developments with potentially devastating consequences. After all, as the Roman General said, "He who desires peace, let him prepare for war."[167] The time to prepare is now.

Notes

[164] Schwartzstein, Stuart J.D., "The Information Revolution and National Security, (Center for Strategic and International Studies Washington D.C.), 1996, p.154.

[165] Xiaoli, Zhu and Zhao Xiaozhuo, *Mei'E Xin Junshi Geming* (The United States and Russia in the New Military Revolution), Beijing, AMS Press, 1996, p. 40-45.

[166] Ibid.

[167] The expression is "Si vis pacam, para bellum" is thought to originates from Caesar's 'De Bello Gallico.' See http://omega.cohums.ohio-state.edu/hyper-lists/classics-1/98-10-01/0070.html.