

NAVAL WAR COLLEGE
Newport, R.I.

DIMINISHING THE CRITICAL VULNERABILITY OF SPACE

by

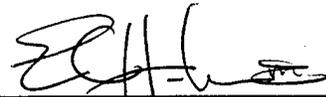
E.C. Helme, III

Lieutenant Commander, United States Navy

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

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

Signature: _____



13 February 1998

19980709 027

DTIC QUALITY INSPECTED 1

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): DIMINISHING THE CRITICAL VULNERABILITY OF SPACE (U)			
9. Personal Authors: E.C. HELME, III LIEUTENANT COMMANDER, UNITED STATES NAVY			
10. Type of Report: FINAL		11. Date of Report: 13 FEBRUARY 1998	
12. Page Count: 20			
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: SPACE; CRITICAL VULNERABILITY; TECHNOLOGY; INFORMATION; RMA; NETWORK; ASYMMETRY; COMMUNICATION; SATELLITES			
15. Abstract: Network-centric warfare (NCW) relies heavily on the exploitation of space and technology to create a more efficient, effective and responsive form of combat power than is presently available to United States forces. The backbone of NCW is the advanced communication and sensor systems that reside in space. These data paths produce a flow of information that promises a greater military reach, irrespective of force size, and supports an increasing trend toward power projection in an era of diminishing forward bases. Unfortunately, our propensity to levy an increasing number of systems upon the skeleton of space has increased its importance as a target to any potential future adversary. Furthermore, a shift to NCW would mark a potentially dangerous commitment to electronic connectivity in order to assure combat power. This increased risk results from the fragility of space assets because components of our space architecture are assailable with relatively low cost, low technology weapons and tactics. Therefore, if we recognize these assets as a critical vulnerability, how do we reconcile a trend toward increasing our dependence on space? The solution requires an environment of innovation that strives to balance hardware, techniques and skills in such a way that realizes the advantages of network-centric warfare without compromising the combat power of individual platforms. Preserving the capability of platform-centric warfare reduces the vulnerability of space assets and safeguards our ability to mass effects regardless of connectivity.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: C	

Abstract of

DIMINISHING THE CRITICAL VULNERABILITY OF SPACE

Network-centric warfare (NCW) relies heavily on the exploitation of space and technology to create a more efficient, effective and responsive form of combat power than is presently available to United States forces. The backbone of NCW is the advanced communication and sensor systems that reside in space. These data paths produce a flow of information that promises a greater military reach, irrespective of force size, and supports an increasing trend toward power projection in an era of diminishing forward bases.

Unfortunately, our propensity to levy an increasing number of systems upon the skeleton of space has increased its importance as a target to any potential future adversary. Furthermore, a shift to NCW would mark a potentially dangerous commitment to electronic connectivity in order to assure combat power. This increased risk results from the fragility of space assets because components of our space architecture are assailable with relatively low cost, low technology weapons and tactics. Therefore, if we recognize these assets as a critical vulnerability, how do we reconcile a trend toward increasing our dependence on space?

The solution requires an environment of innovation that strives to balance hardware, techniques and skills in such a way that realizes the advantages of network-centric warfare without compromising the combat power of individual platforms. Preserving the capability of platform-centric warfare reduces the vulnerability of space assets and safeguards our ability to mass effects regardless of connectivity.

INTRODUCTION

The United States is on the verge of creating an entirely new region for warfare. Capitalizing on the often-interpreted success of Desert Storm, and enabled by recent technological progress, our military has embarked on the most significant philosophical shift in the conduct of warfighting since the development of *levee en masse* some 200 years ago.¹ This shift for the 21st century centers on the exploitation of space and technology to create a more efficient, effective and responsive type of combat -- network-centric warfare.

The backbone of network-centric warfare is the advanced communications and sensor systems that reside in space. These assets not only provide vital input into the "network" of warfighters, but more importantly, provide the data paths upon which most information must travel. Global vision necessitates global communications. JV2010 acknowledges this fact, wherein superior information propagation is listed as the only capability that spans all four operational concepts of Dominant Maneuver, Precision Engagement, Full-dimensional Protection and Focused Logistics. This information flow technology, presently only available to the United States, promises a greater military reach, even with fewer assets, and supports an increasing trend toward power projection in an era of diminishing forward bases. The Concept for Future Joint Operations (CFJO) elaborates: "Technology should allow units to be more widely dispersed, lighter, more mobile, increasing lethal, and have smaller footprints. . . . The ability to locate high-value, time-sensitive fixed and mobile targets and to destroy them with a high degree of confidence will fundamentally change the conduct of war."²

¹Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare Its Origin and Future" Proceedings, January 1998, 29.

²Joint Warfighting Center, Concept for Future Joint Operations, (Fort Monroe, VA: May 1997) 25.

Network-centric warfare is a logical extension of the concepts articulated by the Chairman in the CFJO. It allows for the massing and force multiplication of limited combat elements anywhere around the globe. It appears to be the solution to several crucial problems facing a smaller United States military in the next century . . . but will network-centric warfare survive the next century?

Our propensity to levy system upon system on the skeleton of space increases its importance to any potential future adversary. In essence, we have exchanged the valued "high-ground" of space for a critical vulnerability which, if denied to us, may leave us deaf, blind and incapable of synchronizing actions that, by our own doctrine and planning, may occur on the other side of the planet. Furthermore, the shift to network-centric warfare marks a potentially dangerous commitment to connectivity in order to assure combat power. Even now, operational commanders are experiencing increased reliance on space systems that directly impact tactical ability. How will these operational commanders, charged with fighting our next war, cope if their flow of information is disrupted or destroyed?

Clearly, the incorporation of information technology in the United States military must proceed. However, rather than focus on technical solutions to technical problems, we as a military must produce and retain a mix of options that incorporates a broad spectrum of hardware, techniques and skills in order to reduce the critical vulnerability of space -- call it high tech, low tech and no-tech. The fundamental tenant of these solutions should be to provide warriors at the operational and tactical level the ability to offset or negate an attack upon our strategic space systems using tools and techniques readily available in theater.

CRITICAL VULNERABILITY

Space assets provide a critical set of abilities to American military operations. Consider the scope of activities that are in some way affected by space based assets. Satellites provide critical surveillance of hostile regions and reconnaissance of specific enemy targets and formations. They provide critical information regarding weather and terrain and aid in the movement of friendly forces to convert these potential obstacles into force advantages. They can provide advanced warning, to United States and coalition forces, of attacks emanating from a variety of weapon systems. Finally, they form the structure by which most of this acquired information is passed, known in current terms as the "information backplane."³

Seven years ago, during Desert Storm, over 90% of U.S. communications inter-theater were supported by military and commercial satellites.⁴ That figure would surely be higher today with the proliferation of systems transmitting large amounts of data, such as Video Tele-Conference (VTC), that simply cannot be sent via any other transmission path, a particular problem for mobile or at-sea units that can not connect to existing terrestrial systems. Therefore, in terms of operational art, space assets are a critical strength to the United States, "a capability that must be considered vital for the accomplishment of a given or assumed mission."⁵ As a former science advisor to President Reagan noted, "even in a very limited war, we would have an absolutely critical dependence on space today."⁶

³Cebrowski and Garstka, 31.

⁴Earl J. Matthews, "U.S. Space Systems: A Critical Strength and Vulnerability," (Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1996), 11.

⁵Milan Vego, *On Operational Art* (Newport: U.S. Naval War College, 1997), 121.

⁶Jeffrey L. Canton, "Joint Warfare and Military Dependence on Space," *Joint Forces Quarterly*, Winter 1995, 49.

Once we acknowledge that space is a critical strength, then we must consider whether or not it is a critical vulnerability. Typically, a critical vulnerability can be derived from a critical strength if the capability is both directly related to a center of gravity (COG) and potentially open to attack . . . or at least insufficiently protected from attack.⁷ In this context, COG refers to a critical mass of strength from which combat power is derived. While not a center of gravity alone, most would agree that space is related to a U.S. COG.

With regard to the composition of a COG, Colonel Lawrence Izzo provides, "The center of gravity represents a concentration of enemy strength. It is the most concentrated aspect of the enemy's combat power; that which is most vital to him in the accomplishment of his operational aims. If you could knock it out directly, it would be the most effective target for your blows."⁸ Joint Publication 3-0 further expounds on the relation between COG and a nation's military ability where it explains that, "[c]enters of gravity are the foundation of capability."⁹ They are those characteristics, capabilities, or locations from which a military force derives its freedom of action, physical strength, or will to fight."¹⁰ Even recognizing that the true U.S. strategic COG may be an intangible property such as National Will, the breadth and scope of United States space operations in shaping and enabling our activities abroad must translate into an inextricable connection with a U.S. COG.

The second issue of determining a critical vulnerability involves assessing our exposure to potential attack by an adversary. Space systems are inherently fragile and may be attacked by numerous, presently feasible, means. Known as "counterspace," these techniques of space asset

⁷Vego, 121.

⁸Lawrence L. Izzo, "The Center of Gravity is Not An Achilles Heel," Military Review, January 1988, 176.

⁹Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3-0) (Washington, DC: February 1, 1995), GL-4.

¹⁰Ibid., III-20.

denial include: Meaconing, Intrusion, Jamming and Interference (MIJI); Directed Energy Weapons (DEW); Electromagnetic Pulse (EMP); orbital interceptors; and attacks against the ground-based telemetry, tracking and command (TT&C) segments.¹¹ While not all forms of attack are available to our potential adversaries, employment of any one technique could provide the desired result of reducing or eliminating access to our space-based architecture. In fact, sophistication is not required to execute a counterspace campaign. For example, the Navstar GPS system has two ground link stations in the United States which maintain exact orbital parameters for the constellation. If both ground segments were eliminated the system would be rendered useless.¹²

To accept the above argument, that space is a critical vulnerability, means that one must recognize space as a lucrative and potential target for our adversary during the next conflict. As explained by Robert Butterworth discussing Desert Storm:

“Satellites made possible the scope of surveillance, timeliness of information, and depth of strike envisioned in theories of the military-technical revolution (MTR). Fighting elements could maneuver as tactically needed or desired, confident that connectivity with supplies and reinforcements would be maintained. Surely no future adversary would repeat Iraq’s apparent disregard of space systems.”¹³

It is for this reason that we must consider means to avert complete reliance on space, separate the issue from force planners and develop techniques and tactics to negate the consequences of a successful counterspace program against the United States.

¹¹Matthews, 5.

¹²Ibid.

¹³Robert L. Butterworth, “The Case Against Centralizing Military Space,” Strategic Review, Summer 1996, 42.

CRITICAL VISIBILITY

The United States and its allies have a long and well-publicized history with regard to space and its effect on military operations. Most speak of Desert Storm as the first “space war.” However, space has played a role in virtually every significant operation since the launching of the Corona systems some 30 years ago and a crucial role (providing data or connectivity irreplaceable through other means), continuously, since Operation EL DORADO CANYON in 1986. As mentioned previously, a war today without space assets would eliminate vital reconnaissance, meteorological, positioning and communication abilities for both military forces and strategic decision makers. Publicity and the accessibility of this knowledge makes these capabilities visible to our global competitors.

Ironically, this pervasive visibility means that our vulnerability will only increase with our success in leveraging technologies like network-centric warfare. This is because increasing asymmetry, apparent to our potential adversaries, will drive these hostile forces to seek alternative methods to defeat the United States, employing skills and tactics in a forum that provides some chance of success. Direct military confrontation will not be the preferred method of combat. With regard to this subject Patrick Garrity of the Los Alamos National Laboratory comments, “No nation is apparently seeking to fully emulate or compete with the American approach to war as demonstrated in Operation Desert Storm. . . . [M]ost . . . are thinking about selectively incorporating technologies . . . in the context of their own national security objectives and military circumstances.”¹⁴ Butterworth adds, “This disparity between the United States and

¹⁴Patrick J. Garrity, Why the Gulf War Still Matters: Foreign Perspectives on the War and the Future of International Security, Los Alamos National Laboratory: Center for National Security Studies, Report No. 16, July 1993, 68-69.

the rest of the world is particularly marked in space. The American program is at least an order of magnitude beyond the others in terms of size, diversity, technical sophistication, and funding; it has remained constantly at the leading edge of space science and applications.”¹⁵ This overt dominance of space, while providing critical capabilities, will dissuade potentially hostile states away from the high-tech battlefield of our choice and encourage exploration of other avenues for attack against U.S. assets -- avenues where vulnerabilities exist.

These potential avenues of approach are numerous. Of those mentioned earlier, DEW and ASAT require a significant investment in science and technology that most of our competitors will be unable and unwilling to afford. MIJI, as opposed to direct attack on orbiting platforms, requires a smaller footprint in terms of the infrastructure needed to support such an attack, while relying on technology more readily available to less developed states and groups. A simple example of this technology may be found in the softball-sized GPS blockers that are capable of disrupting Navstar signals to receivers over an area of miles. At the very end of the technology spectrum and most readily attainable today are attacks on U.S. TT&C segments. These attacks would require only an understanding of the architecture of the targeted system coupled with a terrorist ability already demonstrated in places like New York and Oklahoma City. Steven Lambakis, an analyst in U.S. space policy and space power, discusses this fragility when he says, “. . . if we lack a robust capability to exercise positive control under duress . . . space power cannot be considered much more than a fleeting attribute. Without staying power, space power is a fantasy.”¹⁶

¹⁵Butterworth, 44.

¹⁶Steven Lambakis, “The United States in Lilliput: The Tragedy of Fleeting Space Power,” Strategic Review, Winter 1996, 32.

Accepting that attacks of this nature are both desirable to an adversary and technically feasible, and proposing that the pool of techniques and targets is large and increasing daily, and further recognizing the importance of these capabilities to United States military operations, it stands to reason that the United States should not only continue to develop technically-founded responses to these threats, but should explore other, less technologically dependent means of diversifying our space related abilities. This should include a concerted effort to empower operational commanders with the means to decrease dependence on strategic systems.

LOW-TECH/NO-TECH SOLUTIONS

The global aspect of strategic space systems rightly translates into strategic-level control over those assets. While operational and tactical commanders may be consumers of the products delivered from these platforms, the operation and protection of these capabilities must reside centralized, for efficiency, within the strategic levels of our military and civilian security organizations. Furthermore, the inherent weaknesses of these systems must not be allowed to adversely affect the operational and tactical levels of warfighting. That being the case, the operational commander must be provided with an ability to locally replicate the capabilities provided by space assets, or at least be prepared to accomplish required tasks without those capabilities.

In recognizing this requirement, the military has repeatedly called for some level of control of these strategic systems at the operational level. However, typical proposals usually focus on providing a strategic capability in theater, for example, local orbital launch capability to ensure reconstitution of destroyed/damaged orbiting assets. For the most part, these options have been found to be too expensive. Butterworth explains:

“For most tactical applications, satellites face a number of cost and effectiveness deficits as compared with terrestrial systems. For theater reconnaissance, tactical requirements for look angles and revisit and dwell times usually entail so many satellites that other approaches are cheaper. Modernization is another consideration. The expense of satellite options is primarily in the acquisition and launch periods, while the bulk of the expense for airbreathing systems is generally in operations and maintenance. In general, the longer the period of service being compared, the more relatively attractive are satellites. The longer the time period, however, the more likely it is that new sensor or communication technology will be developed and that users will want it inserted into the fielded system, an option that is economically feasible only with airbreathing systems.”¹⁷

In place of controlling space assets, a closer integration between civilian and military organizations responsible for producing, interpreting and disseminating space-based information has yielded positive results for the local commander. U.S. defense officials say that the air campaign in Bosnia, for example, “showed the greatest strides over the Gulf War experience . . . in providing timely intelligence to the frontline fighter. It has more to do with hooking existing systems up better and faster than with introducing new collection systems.”¹⁸

The problem is that this solution does nothing to reduce the operational and tactical commander’s requirement for satellite connectivity -- the crux of the vulnerability issue. In fact, it only increases his dependence on the information architecture resident in space, the information backplane. Although complete disruption of global communications must be considered remote, recently developed data intensive communications may have to be curtailed if the number or fidelity of some space assets is compromised. Knowing that the commander in the field must be prepared to function with significantly less information than available in peacetime operations produces two divergent courses of action for military planners.

¹⁷ Butterworth, 44.

¹⁸ Bradley Graham, “U.S. Sharpens Combat Picture,” The Washington Post, 27 September 1995, A24.

COURSES OF ACTION

Two general philosophies exist when considering remedies to the above situation of vulnerability and dependence: 1) develop inter-theater systems and techniques that mimic satellite functions and 2) identify, retain and practice those skills that permit the application of combat power while not relying on the "information backplane" of space. These concepts should be encouraged to mature in parallel such that warfighters could identify from practical experience which capabilities are irreplaceable (and therefore require some form of theater-strategic mimic) and which may be addressed through non-technical means.

An example of a mimic might be an ultra-high altitude unmanned aerial vehicle that has the ability to serve as a communications relay across an entire theater, substituting exactly for a strategic satellite asset. Although germane to the issue of decreasing space vulnerability and dependence, these solutions are more effectively explored as force planning initiatives and, therefore, fall beyond the realm of this paper.

The second philosophy, that of leveraging skills and tactics not reliant on space, falls directly under the cognizance of the operational commander and may be practically investigated today since it is not dependent on the advent of new technologies. In fact, the military has years of experience operating in this regime, experience that must not be divested from the fighting forces under the promise of precise and perfect electronic massing of forces and effects.

THE TECHNOCRATIC TUNNEL¹⁹

While technology will be able to offset an appreciable amount of the vulnerability inherent with satellite connectivity, it will not be so impervious as to dissuade potential

¹⁹Gary W. Anderson and Terry C. Pierce, "Leaving the Technocratic Tunnel," Joint Force Quarterly, Winter 1995, 69.

competitors from attacking our space infrastructure. Therefore, future success in battle may one day depend on skills from the past -- those not resident in or associated with space. These skills would center on the operational commander's ability to locally synchronize the activities of his forces using techniques that function irrespective of satellite presence, such as UHF and HF voice and data links. In addition to the simple mechanics required to ensure autonomous action in the absence of the global web of the future, there is an overarching issue of decentralized mission control.

As discussed by Colonel Gary Anderson and Commander Terry Pierce in a recent Joint Force Quarterly article regarding RMAs, military forces today are principally organized in a hierarchy "designed to support highly centralized decisionmaking and close oversight."²⁰ The genesis of this arrangement was a need to synchronize movement and maximize firepower. The expanded connectivity afforded by the advent of the information age and space assets has, so far, served only to promote further the concept of centralized decisionmaking.

For example, much was made of recent Battle Group operations in the Taiwan Straits during a period of heightened tensions with the Peoples Republic of China. The BG Commander was almost instantly able to provide input to and receive guidance from the Seventh Fleet Commander several thousand miles distant, who in turn was able to have similar consultations with CINCPAC, located in Hawaii. While some would herald this as a success story for the information backplane of space, what must be asked is how would these commanders have performed if their communications systems had not been available -- a reasonable scenario for our next major conflict. Can the theater-strategic level of command consistently expect to be

²⁰Anderson and Pierce, 79.

able to directly control the operational-tactical level of warfare and how will the future operational commander function in the absence of this control?

Anderson and Pierce argue that the hierarchical model of the military is ill-suited for the advent of increased information and connectivity. They describe the present network-centric warfare mindset as one of "detail-control that is derived from a desire for certainty, order and precision." The trend toward tighter control of assigned forces, using pathways provided by space and as demonstrated by the confrontation with the Peoples Republic of China, would appear to support their argument.

To counter this trend, military information structures must follow the lead of other complex distributed networks, such as the Internet, and empower distributed nodes while demanding independent action. In the words of Anderson and Pierce, ". . . just as computers have flattened corporate organization structure, the military will likewise have to restructure and rely more on decentralized control."

The heretofore unmentioned dividend of this scheme is that decentralized control -- control that is mission-oriented vice detail-oriented -- will reduce our critical dependency on space because the nodes (ships, aircraft, tanks, etc.) will be enabled to act relatively autonomously once mission tasking and guidance have been received. This will allow U.S. forces to operate with overwhelming superiority in the presence of space assets and effectively in their absence. The crux of the problem is identifying the extent to which the precepts of network-centric warfare should be allowed to supplant traditional methods of massing -- numbers or networks and in what proportion?

THE KEY: NETWORK-CENTRIC WARFARE

In discussing network-centric warfare Vice Admiral Cebrowski is right -- NCW will play a role in producing overwhelming superiority. However, it must not impede combat operations when NCW's crucial data links or space assets have been severed or disrupted. Vice Admiral Cebrowski, discussing common themes in the changes occurring in military affairs, cites as one of those themes, "the shift from viewing actors as independent to viewing them as part of a continuously adapting ecosystem." It is precisely this issue that permits network-centrism to supplant platform-centric warfare, a dangerous trend that weakens the unit commander in any situation less than perfect connectivity. Our goal should be a harmony between maximum unit combat power (empowerment of the node) and the electronic massing of effects to multiply that power (network-centric warfare).

The case to imbue the principles of networking onto the military is a strong one. In his recent Proceedings article Admiral Cebrowski provides examples of businesses that have experimented and succeeded with the application of network centrism.²¹ He draws parallels between competition in the commercial sector and competition among the militaries of the world -- certainly the concepts of increased agility, improved and accurate response to dynamic events and a preference toward self-synchronization (a.k.a. bottom-up synchronization) are all lucrative goals for any organization. His examples, Walmart, the retailing giant, and Deutsche Morgan Grenfell, a securities brokerage house, have embraced networked operations and reaped benefits as indicated by dominance (full spectrum dominance?) in their particular markets.

²¹Cebrowski and Garstka, 30.

The tragic flaw, the reason why the power of the node must remain credible, the reason why alternatives to space-centered networking must be provided to the operational commander can be deduced not in what Admiral Cebrowski says about NCW, but in what he doesn't say about NCW. In all of the successes he cites, not once does he address the ramifications of physical attack by a competitor to the net or its methods of transmission. Of course, in the commercial world, such strategies are contrary to accepted operating practices -- would K-Mart contemplate a concerted attack on Walmart's network system? Probably not. However, in military operations such an attack would not only be acceptable, but prudent. The rules of business, while similar, do not universally apply to the military. Our space-based architecture will likely be attacked in the next conflict and to fully leverage our combat ability upon an area of questionable resiliency is simply dangerous.

RECOMMENDATIONS

The answer is balance. Recognizing the sound underpinnings of network-centric warfare we must develop an ability to mass combat effects electronically, over an entire theater or around the globe. Additionally, we should expand systems like the Cooperative Engagement Capability (CEC) that allow tactically-oriented formations to do the same. Concurrent with the maturation of NCW, and most importantly, we must preserve the ability of individual units to function both within a network system and independently, under more autonomous circumstances than those provided by presently envisioned systems. Also, as we improve platforms for operations on this new plane of warfare we must be vigilant of the propensity toward decreased effectiveness of pre-existing forces.²²

²²Jeffrey A. Harley, "Information, Technology, and the Center of Gravity," Naval War College Review, Winter 1997, 84.

Our view of space and its accessibility to the warfighter must also change. Rather than the panacea for all of our communications challenges, space must be considered a critical vulnerability and other paths for data transfer between warfighting nodes must be explored. This should include less exotic links that rely on UHF and HF propagation, perhaps interfacing with terrestrial systems (e.g. fiber optic cables) and commercial transoceanic systems to provide global coverage. Creating more robust "grids" (information, sensor and engagement)²³ and divesting critical circuits from space will, by reducing its attractiveness to potential attackers, serve to decrease its vulnerability.

Finally, we should strive to preserve and promote the commander's ability to operate with less information, and thereby avoid the development of a generation of commanders unable to be weaned from the information backplane, should the day ever arise when the "system of systems" is not available to our forces. We must not forget that "technology cannot change the fact that attempting to forcibly inflict one's will on a determined foe is an inherently dangerous, bloody, chaotic endeavor."²⁴ This requires a level of training, exercise, and doctrine development commensurate with the challenges of both an information-rich and an information-poor environment.

CONCLUSION

The United States has never before wedded itself with such determination to the concept of superior information. Granted, technology previously limited what could be reasonably

²³"Information Paper: Observations on the Emergence of Network-Centric Warfare."
<<http://www.dtic.mil/jcs/j6/education/warfare.html>> (20 December 1997), 2.

²⁴David Adams, "We Are Not Invincible," Proceedings, May 1997, 36.

expected. However, beyond technological capability, there is a pervasive belief that information push/pull will be available, as it was during Desert Storm, in the next war.

So pervasive is this belief that the success of employing our newest weapons will depend heavily on the presence of a complex and fragile satellite architecture. Notably, the weapons themselves require satellite-provided information to fully utilize their designed capabilities. The mindset of the military is dangerously changing. Where wars were once fought with or without information and sound military strategy assumed that an information void would exist, we are now confining our options to operations reliant upon the critical vulnerability of space.²⁵ Moreover, we have developed and proven for the world the utility of targeting and systematically destroying hubs of information.

Taken together we have built the foundations of a complex system assailable by our global competitors. However, instead of seeing the folly in limiting our options to this skeleton, the goals of network-centric warfare are simply too tantalizing: clearing the fog of war; operating with such agility and precision as to deliver the decisive blow before the enemy even fully realizes he is engaged; maximizing the potential of a smaller, leaner force; reaching deeper into competitor's strategic infrastructures than ever before.

Unfortunately space, information, and network-centric warfare are all intrinsically linked and carry both the promise of incredible military superiority and the burden of obvious vulnerability. How we elect to balance capability and vulnerability will determine the viability of these systems in the next inevitable conflict.

²⁵Alan D. Campen, "Assessments Necessary in Coming to Terms with Information Warfare," *Signal*, June 1996, 48.

BIBLIOGRAPHY

- Adams, David. "We Are Not Invincible." Proceedings, May 1997, 35-39.
- Air University Air Command and Staff College. Space Handbook: A War Fighter's Guide to Space, December 1993.
- Anderson, Gary W. and Terry C. Pierce. "Leaving the Technocratic Tunnel." Joint Force Quarterly, Winter 1995, 69-75.
- Becher, Klaus. "Space Technology as a Factor of International Stabilization and Destabilization." Space Policy, November 1995, 233-238.
- Butterworth, Robert L. "The Case Against Centralizing Military Space." Strategic Review, Summer 1996, 41-49.
- Campen, Alan D. "Assessments Necessary in Coming to Terms with Information Warfare." Signal, June 1996, 47-49.
- Caton, Jeffrey L. "Joint Warfare and Military Dependence on Space." Joint Force Quarterly, Winter 1995, 48-53.
- Cebrowski, Arthur K. and John J. Garstka. "Network-Centric Warfare Its Origin and Future." Proceedings, January 1998, 28-35.
- Estes, Howard M. "Sustaining the Strategic Space Advantage." Defense Issues, vol. 12, no. 15.
- Fulghum, David A. and Joseph C. Anselmo. "DARPA Pitches Small Sats for Tactical Reconnaissance." Aviation Week & Space Technology, 09 June 1997, 29-31.
- Garrity, Patrick J. Why the Gulf War Still Matters: Foreign Perspectives on the War and the Future of International Security. Los Alamos National Laboratory: Center for National Security Studies, Report No. 16, July 1993, 68-69.
- Graham, Bradley. "U.S. Sharpens Combat Picture." The Washington Post, 27 September 1995, A24.
- Hamon, Dale R. and Walter G. Green. "Space and Power Projection." Military Review, November 1994, 61-67.
- Harley, Jeffrey L. "Information, Technology, and the Center of Gravity." Naval War College Review, Winter 1997, 66-87.
- "Information Paper: Observations on the Emergence of Network-Centric Warfare."
<<http://www.dtic.mil/jcs/j6/education/warfare.html>> (20 December 1997).

Izzo, Lawrence L. "The Center of Gravity is not an Achilles Heel." Military Review, January 1988, 72-77.

Kaminski, Paul G. "Outside-the-Box Thinking Needed." Defense Issues, vol. 12, no. 5.

Lambakis, Steven. "Exploiting Space Control." Armed Forces Journal International, June 1997, 42-46.

Lambakis, Steven. "The United States in Lilliput: The Tragedy of Fleeting Space Power." Strategic Review, Winter 1996, 31-42.

Matthews, Earl J. "U.S. Space Systems: A Critical Strength and Vulnerability." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1996.

Phillips, Theresa M. "Space Support at the Operational Level: How Have We Learned the Lessons From Desert Storm?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1996.

Rowe, Jeffrey. "U.S. Space Command: Managing Critical Assets in Space and on the Ground." Defense Electronics, March 1992, 35-45.

"Space Almanac." Air Force Magazine, August 1996, 28-49.

Sweetman, Bill. "Spy Satellites: The Next Leap Forward." Jane's International Defense Review, January 1997, 26-32.

Thomson, Allen. "Satellite Vulnerability: A Post-Cold War Issue?" Space Policy, February 1995, 19-30.

Tirpak, John A. "Future Engagement." Air Force Magazine, January 1997, 18-23.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations (Joint Pub 3-0) Washington, DC: 1 February 1995.

Vego, Milan. On Operational Art. Newport: U.S. Naval War College, 1997.