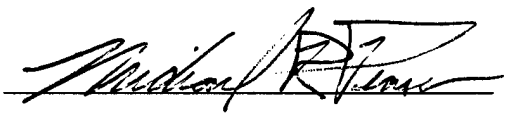
NAVAL WAR COLLEGE
Newport, R.I.

INFORMATION SUPERIORITY: "WHERE'S THE BEEF?!"

by
Michael R. Pease
Lieutenant Commander, United States Navy

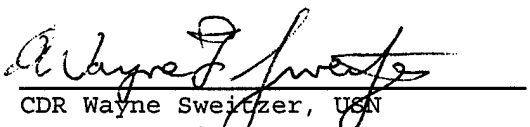
A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

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

Paper directed by Captain G. Jackson
Chairman, Joint Military Operations Department



12 FEB 98
Date

CDR Wayne Sweitzer, USN
Faculty Advisor
Raymond A. Spruance Military Chair of
Command, Control, Communications,
Computers, and Intelligence (C4I)

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority: UNCLASSIFIED	
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: Naval Command and Staff College	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): Information Superiority: "Where's the Beef?!" (U)	
9. Personal Authors: Lieutenant Commander Michael R. Pease, U.S. Navy	
10.Type of Report: FINAL	**11. Date of Report:** 13 Feb 98
12.Page Count: 22	
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: information superiority C4 ISR Joint Vision 2010 CFJO imagery SIGINT	

15. Abstract: *Joint Vision 2010* rests on the assumption that U.S. forces will enjoy "dominant battle space knowledge" or "information superiority" over any potential adversary by 2010. Proponents of *Joint Vision 2010* point to the benefits of reducing the fog of war without justifying their underlying premise. Can future JTF commanders count on information superiority?

While *Joint Vision 2010* points to the many positive trends in information technology and friendly C4, this is only half of the information superiority problem. Information superiority also includes Intelligence, Surveillance and Reconnaissance (ISR). The nature of C4 information fundamentally different from that of ISR. While information age advances tend to favor improved C4, they can seriously hinder ISR.

The end of the cold war and the rise of the information age pose serious challenges to ISR. In most areas and levels of imagery, signals and human ISR, the current state and trends do not guarantee information superiority in 2010.

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

INFORMATION SUPERIORITY: "WHERE'S THE BEEF?!"

Joint Vision 2010 rests on the assumption that U.S. forces will enjoy "dominant battle space knowledge" or "information superiority" over any potential adversary by 2010. Proponents of *Joint Vision 2010* point to the benefits of reducing the fog of war without justifying their underlying premise. Can future JTF commanders count on information superiority?

While *Joint Vision 2010* points to the many positive trends in information technology and friendly C4, this is only half of the information superiority problem. Information superiority also includes Intelligence, Surveillance and Reconnaissance (ISR). The nature of C4 is fundamentally different from that of ISR. While information age advances tend to favor improved C4, they can seriously hinder ISR.

The end of the cold war and the rise of the information age pose serious challenges to ISR. In most areas and levels of imagery, signals and human ISR, the current state and trends do not guarantee information superiority in 2010.

Table of Contents

Introduction

From Admiral Owen's "*System of Systems*"[1] to JCS's "*Concept for Future Joint Operations*" (*CFJO*)[2] "dominant battle space knowledge" or "information superiority" has become prerequisite for future joint operations. Information superiority enables dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. The presumption that future U.S. forces will enjoy information superiority to achieve full spectrum dominance is the basis for *Joint Vision 2010*[3]. Far from being just a fashionable term, the postulate of future information superiority could drive important acquisition, doctrine, training, strategic, operational and tactical decisions. With so much riding on a single assumption where is the corresponding justification -- "Where's the Beef?!"

The latest and most specific definition of JCS's "conceptual framework for America's armed forces"[4], *CFJO*, offers little support to its information superiority hypothesis. While potential threats are mentioned, none are said to be able to negate the vision. *CFJO* acknowledges a contest for information superiority but concludes:

> "Although we will continue to achieve new levels of technological capability, *[Joint Vision 2010's]* prediction that while 'the friction and the fog of war can never be eliminated, new technology promises to mitigate their impact' will remain true."[5]

In other words, threats to technology based information superiority will be mitigated by superior technology. Far from defending the information superiority postulate - *CFJO* evades the issue behind a cloak of technical hubris. Absent official substantive support for the information superiority assumption how valid is *Joint Vision 2010*?

Operational Information Duality

A military commander is principally concerned with two types of information in the pursuit of dynamic battlespace awareness-- (1) friendly force information, and (2) enemy force information. Understanding the differences between these two categories of operational information is critical to appreciating the extent of *Joint Vision 2010's* optimistic information superiority supposition.

Own force information is gained through **collaboration.** Dispersed friendly units share state and control data through a complex "network of networks."[6] Because own force information is collaborative, increased technology and resources can directly improve *own force* situational awareness. Though friendly forces can still contribute to the "fog of war", *CFJO's* contention that technology improvements will improve a commander's view of the battlespace[7] should at least hold true for friendly forces.

Conversely, **information about the enemy** involves **competition.** Intelligence, Surveillance and Reconnaissance (ISR) assets compete against enemy information security and deception measures for access to relevant data. For a commander to enjoy enemy situation awareness two conditions must be satisfied:

1) Friendly forces must be able to collect and exploit relevant information.

2) The enemy must be unable or unwilling to either protect his relevant information, or deceive friendly forces.

In the real world, ISR involves a never ending battle between an enemy trying to deny critical information and friendly forces attempting to

collect, validate, integrate and exploit it. Like other areas of conflict, denial is often easier than control. Protecting one's own information is usually simpler than obtaining enemy information. So, unlike the omniscient C4 envisioned in *CFJO*, evolving ISR technology and resource advantages will not necessarily translate to superior knowledge of the enemy.

CFJO ignores or downplays this distinction between friendly and enemy information. In fact, *CFJO* created an "information superiority construct"[8] that no longer refers to such doctrinal information elements as communications, computers, intelligence, reconnaissance, surveillance, and information warfare. The combined term C4ISR:

> "generally used to describe all of the systems and functions associated with the command and control system and intelligence function...is not useful within the CFJO information superiority construct..."[9]

The new construct divides information superiority into information systems, relevant information, and information operations. This more general view of battlespace awareness hides previously suggested distinctions between friendly and enemy information.

Few argue that the U.S. military's C4 technology and resource advantage will disappear by 2010. Except for the possible emergence of effective RF weapons, conventional forces should be able to protect their own force awareness to the extent required by *Joint Vision 2010*. Unfortunately, U.S. forces do not enjoy the same ability to control information in the ISR arena. Improved knowledge of the enemy requires not only more and better assets, but also cooperative adversaries to be exploited. Therefore, to judge the validity of JV 2010's information superiority assumption one should look at ISR trends and ask two

questions:

1) Will future ISR assets be able to deliver enough relevant information to satisfy the demands of dominant maneuver, precision engagement and full dimensional protection?

2) Can future adversaries deny enough critical information to counter dominant maneuver, precision engagement and full dimensional protection?

Imagery

U.S. forces should continue to enjoy advances in imagery ISR technology, most notably at the tactical level in surveillance. JSTARS and UAVs have shown significant promise in many applications. JSTARS provides a view of ground targets that choose to move, based on doppler radar processing technology. Limiting factors include line of sight, and the enemy's ability/willingness to jam, deploy decoys, or move at speeds insufficient to register on the doppler radar of the JSTARS aircraft. As a large high value unit, JSTARS must operate outside of any threats. Though it can't positively identify most objects, JSTARS has become a valuable heuristic tool to cue other assets. In 2010 multiple detections by different types of sensors, followed by sophisticated data fusion methods, may be needed for positive identification in the face of determined enemy countermeasures. Positive identification should continue to be a prerequisite for precision engagement, both to meet rules of engagement criteria and justify use of expensive weapons.

UAVs should increasingly provide joint forces much needed resources to find, identify and even illuminate enemy targets. On the

other hand, enemy targets and their signatures are becoming smaller and, in some cases, ambiguous. Coastal defenses, for instance, are no longer large, semi-fixed sites. Cruise missile components are smaller, more mobile, and more easily concealed. Is that a civilian truck or missile transporter? Will there be enough UAVs, or other platforms and sensors, to detect and identify contacts of interest?

At the tactical level both JSTARS and UAVs provide a great improvement over the status quo, but the views from other levels of war and branches of ISR are not as promising. Current states and trends in many parts of the ISR arena don't support the notion of assured information superiority in 2010.

Imagery support at the operational and strategic level faces daunting challenges. The explosion of sophisticated commercial satellite imagery systems will soon give everyone, including potential enemies, access to cheap high resolution imagery products.[10] Future foes will know the strengths and weaknesses of overhead imagery. They will appreciate the need for, and could effectively develop and test, multi-spectral concealment and deception measures.

As "weapons of precise destruction"[11] (WPD) (i.e. smart weapons) proliferate along with weapons of mass destruction, the strategic and operational imagery problem escalates. Enemy military centers of gravity in the information age will shrink in footprint, and grow in number by using distributed small mobile assets rather than a few fixed large targets, while the area to move and hide such entities will grow. The modern enemy will enjoy many home field advantages plus the added benefits of smaller, more lethal tools. Modern cruise missiles, mobile

ballistic missiles and SAMs increase an enemy's capabilities while confounding imagery assets. Many potential adversaries are already looking to increase mobility and decrease footprint for that very reason.

> "First, China must improve the survival ability of its strategic nuclear weapons. [General Fu Quanyou] writes, 'We should strengthen research on small, solid fuel and highly automated mobile missiles'..."[12]

Conversely it is harder to hide major U.S. force projection assets in a foreign region.

The trend in imaging satellite vulnerability is also troubling. Today imagery satellites are easily identified and tracked by space buffs and amateur astronomers with personal equipment. Space launches are openly announced. Their ephemeris data are openly shared on the INTERNET for all to see.[13] By gathering and exploiting this information, hostile countries can minimize imaging satellite exposure. Adversaries may simply limit sensitive activity during imaging satellite passes. In addition to passive cover and deception measures many hostile forces will likely be able to engage imaging satellites with active countermeasures.

Active countermeasures require more precise tracking, but modern technology proliferation makes this much easier. Today several developed countries can accurately track low earth orbiting (LEO) imagery satellites by radar using old technology and relatively small investment.[14] Space tracking radars are in the hands of potential adversaries or their allies as part of their rocket programs. With tracking data from radars, satellites can be engaged by electromagnetic devices.

As imaging sensors become more sensitive they become more vulnerable to jamming by various emitters. With enough well aimed laser energy, charge couple devices may be vulnerable to temporary or permanent laser "blinding." Though more costly and probably not yet feasible, future enemies could conceivably develop a direct assent LEO anti-satellite rocket capability[15].

Even if LEO imaging satellites are permitted unfettered operations over hostile territory, other challenges remain that are not addressed by *Joint Vision 2010* advocates. Military imagery exploitation is, and will likely remain, an information speed bump[16]. Imagery analysis requires many highly skilled professionals with years of specialized training and experience. Digital processing advances have improved productivity and access, but the need for expensive and time consuming human exploitation remains. Artificial intelligence, long touted as a potential solution to a shortage of analysts, has yet to pay off.

While the supply of exploitation assets shows no sign of significant improvement, demand for imagery products will likely explode. As the market for commercial imagery products continues to grow, the U.S. government will have to compete for more expensive analytical talent. Concurrent advances in weaponry and greater U.S. engagement around the world has increased the demand for fast high quality imagery exploitation. To stay inside an opponent's decision cycle more imagery specialists will be needed to interpret more images in less time. Within the national intelligence community itself, growing competition for scarce resources will effect the availability of analysts to support the military. Monitoring environmental concerns,

economic activity, disaster relief, refugee flow, law enforcement targets, narcotics trade, terrorism, weapons proliferation and treaty compliance, will compete with strategic, operational and tactical military intelligence requirements.[17]

Signals

Perhaps the greatest threat to future information superiority lies in the potential defeat of signals ISR.

> "Secure cryptography widely available outside the United States clearly has an impact on national security interests including economic, military, and political."[18]

Nowhere else has information technology growth improved a potential adversary's ability to conceal relevant information and deceive intelligence efforts. This is because the information revolution significantly improves the prospects for information security.

> "Protection and security measures are broader than the U.S. concepts of operations security (OPSEC) and force protection. The [opposition force] considers information a critical resource and takes appropriate protective measures such as censoring, camouflage, counter-reconnaissance, and encryption."[19]

The same technology that enables better C4 can also limit ISR.

As digital communications costs continue to drop, more countries are replacing old vulnerable analog systems with more sophisticated low probability of intercept (LPI) digital products. Fiber optic lines are replacing radio relay systems. Though the proliferation of cellular telephony creates more signals for potential exploitation, they are often harder to collect. Older analog cellular is quickly going digital. Cellular signals are relatively low power and interfere with each other outside of each "cell." The combination of terrain, low

power, spread spectrum techniques and overlapping signals competing for limited bandwidth increase the collection problem.

> "The ability to filter through the huge volumes of data and to extract the information from the layers of formatting, multiplexing, compression, and transmission protocols applied to each message is the biggest challenge of the future. Increasing the amounts and sophistication of encryption add another layer of complexity."[20]

As voice and data become digital they become easy to encrypt. The revolution in computer technology and advances in number theory have made strong encryption easy to employ, reliable, and normally impractical to attack. In a closed session of the House Committee on International Relations, Deputy Director of the National Security Agency, William Crowell, commented on simple encryption's effectiveness saying,

> "...[private cryptologists] last week broke a single message using 56-bit DES. It took 78,000 computers 96 days to break one message, and the headline was, DES has weak encryption. [FBI director Freeh] doesn't consider that very weak. If that had been 64-bit encryption, which is available for export today, and is available freely for domestic use, that same effort would have taken 7,000 years. And if it had been [strong encryption] it would have taken 8.6 trillion times the age of the universe."[21]

Strong data and voice encryption software, such as "PGP" (Pretty Good Privacy) and "PGP fone", is easy to use and available free on the world wide web.

Even if the U.S. eventually breaks strong encryption, computer technology has now made **totally secure** communications practical. "One-time pad" encryption has and always will be impossible to break, but until the advent of computers, it was difficult to do. Today CD-ROM technology coupled with better random number generators, has made large one-time key pads easy to create, duplicate, and employ.

Besides encryption, critical information now can be readily hidden within "noise." Information can be cloaked in the ones and zeroes that define a picture, or buried within data frames used to send voice or data through a network.

HUMINT

Ironically, as information technologies advance, HUMINT requirements remain high. The "Strategic Intelligence Reviews" of 1994 rated HUMINT as the most important source, "judged to make a 'critical' contribution towards 205 of the 376 intelligence needs identified."[22] Even so, HUMINT has probably faced the most drastic down sizing of all the intelligence sources.

Congress has mandated deep cuts to the clandestine service. Since 1990 the CIA's directorate of operations has lost more than thirty percent of its HUMINT collectors[23]. Many foreign stations have been eliminated or reduced in size.

The military impact of such cuts may never be known, but it is potentially great. Clandestine operations, unlike other forms of ISR, do not usually provide near real time information. Results may take months or years to cultivate, but that does not mean they are insignificant. Throughout history, clandestine operations have yielded significant victories in the quest for critical enemy information. Without HUMINT the breaking of the German enigma code would not have been possible.[24] Only human sources could reveal the nature and extent of Iraq's NBC weapons programs. Clandestine operations may be the only way to tap into otherwise protected or low probability of intercept (e.g. directional or low power) enemy communications.

Resources

While HUMINT has taken the greatest percentage cut within the ISR community it is by no means alone. Since 1989 the budget for intelligence has reportedly dropped 21% in real terms.[25] Congressional and private organizations forecast steady funding, in real terms, for intelligence for the remainder of the century. Beyond 2000 congressional observers see "downward pressure on spending will continue for the foreseeable future."[26] Ironically, greater cuts could hasten much needed reforms.

With a few exceptions, ISR bureaucracies (national and military intelligence organizations) have been much slower than private industry to embrace information age organizational changes. Private firms adapt or die. Companies like IBM and AT&T have already had to make huge changes to compete in the information market. ISR bureaucracies, though facing gradual cuts, still enjoy specialized information monopolies that ensure their continued existence. Imagery, the last competitive intelligence market, was recently consolidated into a single organization called NIMA. Hierarchical structures characteristic of the industrial age dominate many ISR agencies and most military units. Though better communications has improved speed and access to ISR information, that information is still created and controlled by industrial age organizations. Consequently, national and military ISR bureaucracies do not show the same rate of product improvement as their information oriented, market driven counterparts.

Another negative trend that may effect ISR is the erosion of U.S. leadership in high end computing. Japanese companies have replaced

several U.S. companies in the super computer business. Already Japan has caught up with, Cray in processing power.[27] While the mid-range market grows, the high end computer market has stalled. Analysts fear these trends will limit the U.S.'s future remote sensing exploitation and ability to break publicly-available encryption.[28]

Operational Impact

What if JV 2010's information superiority premise is incorrect and future JTF commanders find themselves without enough information about the enemy to support full spectrum dominance? How would lack of ISR information effect U.S. forces at the operational level?

Perhaps the greatest impact would be in the ability to "quickly and accurately identify centers of gravity (COG) and decisive points and assess the best ways and means for simultaneously attacking them in depth."[29] In Iraq and North Korea, for instance, we have seen how well concealed weapons of mass destruction (WMD) programs can limit a Joint Force Commander's ability to identify centers of gravity. It was only through a fortunate defection and aggressive inspection, not routine ISR, that the U.N. learned about Saddam's previously unknown WMD assets.

Even if an enemy COG can be identified, it must be visible at the right time for dominant maneuver and precision engagement. Direct approach to a COG may be problematic without information superiority. For example, despite an extremely permissive ISR environment coalition forces can't directly approach and "precisely engage" Saddam's remaining WMD. A JFC who lacks information superiority may have to pursue a more costly indirect approach, or attack another less attractive COG.

Anticipation of enemy options or actions could also be hampered by

a lack of information superiority. An adversary with effective information security could mask his real intentions. Using deception, the smart adversary could also feed false intentions to receptive ISR assets. Commanders counting on information superiority may be more inclined to take the bait of enemy deceit, especially if it's delivered on a sophisticated ISR platter.

Just as enemy information denial can hinder a commander's ability to leverage the JTF's strengths, it can also allow the enemy to leverage his strengths. Since the end of the cold war, U.S. power projection has relied on higher concentrations of force and fewer numbers of major platforms, bases and ports. Regional powers may be able to leverage newer conventional weapons advantages against these reduced numbers of more vulnerable U.S. high value assets. More easily detected U.S. force concentrations could be engaged by harder-to-find precision standoff weapons.[30]

Conclusion

Contrary to conventional thought, effective information superiority in 2010 may be the exception vice the rule. Intelligence, surveillance and reconnaissance problems appear to be growing, not shrinking - getting harder, not easier. As information intensive weapons and operational concepts dramatically increase friendly ISR requirements, ISR resources to satisfy those requirements are stagnant or declining. Compounding the challenges is the fact that new technologies tend to make it cheaper for 2010 adversaries to protect their critical information and more expensive for us to obtain it.

While the U.S. technology leadership can improve and protect

information systems, it cannot control access to critical enemy information. Ultimately, other factors beyond technical competency will govern ISR performance and battlespace awareness. These factors, properly applied, could deny information superiority and future U.S. operational success. "When you are ignorant of the enemy but know yourself, your chances of winning and losing are equal."[31]

Proponents of the new vision fail to see the growing potential of information denial to counter full spectrum dominance. They count on information asymmetries to provide the leverage for future force projection. Unfortunately equal or superior C4 is not enough. Without sufficient ISR information, the JFC has only half the picture.

Advanced ISR resources may not be enough if they are denied access to relevant information. Though some trends could be reversed to improve U.S. ISR capabilities, that probably won't be enough to overcome increasingly probable enemy countermeasures.

Given a preponderance of the evidence for a future that favors relevant information security we should question the very premise of information superiority in 2010. Before committing to the quest for full spectrum dominance we must consider the effect of information denial on forces and doctrine shaped by *Joint Vision 2010*.

Notes

[1] Admiral William A. Owens, "The Emerging System of Systems," Proceedings, May 1995, 36-39.

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

[3] Joint Chiefs of Staff, Joint Vision 2010, (Washington, D.C.: July 1996).

[4] Concept for Future Joint Operations, 3-5.

[5] Ibid., 45.

[6] JCS J6. "Observations on the Emergence of Network-Centric Warfare." <http://131.84.1.34/jcs/j6/education/warfare.html> (21 November 1997).

[7] Concept for Future Joint Operations, 39.

[8] Ibid., 85.

[9] Ibid., 83.

[10] Graham T. Richardson and Robert N. Merz. "High-Resolution Commercial Imagery and Open-Source Information: Implications for Arms Control." Arms Control and Disarmament Agency Intelligence Brief. 13 May 1996. <http://www.fas.org/irp/ offdocs/acda.htm> (10 December 1997).

[11] David Blair, "How to Defeat the United States: The Operational Military Effects of the Proliferation of Weapons of Precise Destruction," in Fighting Proliferation: New Concerns for the Nineties ed. Henry Sokolski (Maxwell AFB: Air University Press, 1997), 76.

[12] National Defense University. "Chinese Views of Future Warfare." Institute for National Strategic Studies Summaries of the Articles. <http://www.ndu.edu/ndu/inss/books/chinview/ chinasum.html> (12 December 1997).

[13] "Satellite Vulnerability: a post-Cold War issue?" Space Policy. February 1995, 19-30) <http://www.fas.org/spp/eprint/ at_sp.htm> (19 December 1997).

[14] Ibid.

[15] Ibid.

[16] Congress, House, Permanent Select Committee on Intelligence, IC21: Intelligence Community in the 21st Century, Staff Study (Washington: U.S. Govt. Print. Off., 1996), 131.

[17] National Defense Panel, Transforming Defense: National Security in the 21st

Century, Report (Arlington, VA, 1998), 63,64.

[18]Michael S. Conn, NSA Information Policy Chief,"National Security Agency Central Security Service Letter, Serial: Q43-11-92 0", 10 June 92, <http://www.eff.org/pub/Privacy/ Crypto_misc/nsa_abernathy.answers> (10 December 1997).

[19]MAJ Erin J. Gallogly-Staver and MAJ Raymond S. Hilliard, "Information Warfare: OPFOR Doctrine - An Integrated Approach", Military Intelligence Professional Bulletin, (12 December 1997).

[20]IC21: Intelligence Community in the 21st Century, 121.

[21]William P. Crowel, U.S. Congress, House, Committee on International Relations, Members Briefing Regarding Encryption, Hearing before the Committee on International Relations, ___ Cong., ___ sess., 26 June 1997, <http://jya.com/hir-hear.htm> 01 (February 1998).

[22]IC21: Intelligence Community in the 21st Century, 186.

[23]Ibid., 193.

[24]Members Briefing Regarding Encryption.

[25]Commission on the Roles and Capabilities of the United States Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence, Report (01 March 1996, Govt. Print. Off., Washington, D.C.) <http://www.milnet.com/ milnet/usint/int017.htm> (30 January 1998)

[26]Ibid., <http://www.milnet.com/milnet/usint/int003.htm>

[27]National Coordination Office for Computing, Information, and Communications, "High End Computing for National Security," April 1997, <http://www.hpcc.gov/talks/ipt-02Apr97/ slide04.html> (08 January 1998).

[28]Ibid.,<http://www.hpcc.gov/talks/ipt-02Apr97/slide13.html>.

[29]Concept for Future Joint Operations, 62.

[30]Fighting Proliferation: New Concerns for the Nineties, 77.

[31]Sun Tzu, quoted in Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations (Joint Pub 2-0) (Washington, D.C.: 05 May 1995), IV-14.

Bibliography

Anderson, Gary W. and Terry C. Pierce. "Leaving the Technocratic Tunnel," Joint Force Quarterly, Winter 95-96, 69-75.

Berner, Steve. "Proliferation of Satellite Imaging Capabilities: Developments and Implications," in Fighting Proliferation: New Concerns for the Nineties ed. Henry Sokolski (Maxwell AFB: Air University Press, 1997), 95-129.

Blair, David. "How to Defeat the United States: The Operational Military Effects of the Proliferation of Weapons of Precise Destruction," in Fighting Proliferation: New Concerns for the Nineties ed. Henry Sokolski (Maxwell AFB: Air University Press, 1997), 75-94.

Commission on the Roles and Capabilities of the United States Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence, Report (01 March 1996, Govt. Print. Off., Washington, D.C.) <http://www.milnet.com/ milnet/usint/int017.htm> (30 January 1998)

Conn, Michael S.."National Security Agency Central Security Service Letter, Serial: Q43-11-92 0", 10 June 92, <http://www.eff.org/pub/Privacy/ Crypto_misc/nsa_abernathy.answers> (10 December 1997).

Crowel, William P. U.S. Congress, House, Committee on International Relations, Members Briefing Regarding Encryption, Hearing before the Committee on International Relations, ___ Cong., ___ sess., 26 June 1997, <http://jya.com/hir-hear.htm> 01 (February 1998).

Crypt Cabal. "Cryptography FAQ," <http://www.landfield.com/faqs/cryptography-faq/part01/>, 18 January 1998.

Defense Science Board, Improved Application of Intelligence to the Battlefield, May-July 1996. <http://www.fas.org/irp/program/ dsb_battlfield_rep.htm>

Federation of American Scientists. "PDD-35 Intelligence Requirements." Washingtion: 2 March 1995. <http://www.fas.org/irp/offdocs/pdd35.htm>.

Gallogly-Staver, Erin J., and MAJ Raymond S. Hilliard. "Information Warfare: OPFOR Doctrine - An Integrated Approach", (Military Intelligence Professional Bulletin, 12 December 1997) <http://call.army.mil/call/ nftf/sepoct97/infowar.htm>.

JCS J6. "Observations on the Emergence of Network-Centric Warfare." <http://131.84.1.34/jcs/j6/education/warfare.html> (21 November 1997).

Johnson, Stuart E. and Martin C. Libicki., ed., Dominant Battlespace Knowledge, Washington: National Defense University, 1996.

Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations (Joint Pub 2-0) Washington, D.C.: 05 May 1995.

Joint Chiefs of Staff, Joint Vision 2010, Washington, D.C.: July 1996.

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

National Coordination Office for Computing, Information, and Communications, "High End Computing for National Security," April 1997, <http://www.hpcc.gov/talks/ipt-02Apr97/ slide04.html> (08 January 1998).

National Defense Panel, Transforming Defense: National Security in the 21st Century, Report (Arlington, VA, 1998)

Owens, William A., "The Emerging System of Systems," U.S. Naval Institute Proceedings, May 1995.

Pillsbury, Michael. Chinese Views of Future Warfare, (Washington: National Defense University, 1997) <http://www.ndu.edu/ndu/inss/books/ chinview/chinasum.html> (12 December 1997).

Reno, Janet, to Member of Congress, 18 July 1997 <http://www.jya.com/crypto-law8.htm>

Richardson, Graham T. and Robert N. Merz. "High-Resolution Commercial Imagery and Open-Source Information: Implications for Arms Control." Arms Control and Disarmament Agency Intelligence Brief. 13 May 1996. <http://www.fas.org/irp/ offdocs/acda.htm> (10 December 1997).

Smith, Edward A., Jr. "Putting It Through the Right Window," U.S. Naval Institute Proceedings, June 1995, 38-40.

Staten, C. L. "Strategic Knowledge; Preventing the Bombing of the Bridge to the 21st Century" Chicago, Emergency Response & Research Institute: 9 April 1997 <http://emergency.com/stratknw.htm>.

Sattler, Michael. "Steganography," (13 November 1995) <http://www.indstate. edu/msattler/s.../privacy/topics/steganography.html> 01 February 1998.

Thomson, Allen. "Satellite Vulnerability: a post-Cold War issue?" (Space Policy. February 1995, 19-30) <http://www.fas.org/spp/eprint/ at_sp.htm> (19 December 1997).

U.S. Army. "Army Vision 2010: Information Superiority," <http://www.army.mil/ 2010/information_superiority.htm>.

U.S. Congress, House, Permanent Select Committee on Intelligence, IC21: Intelligence Community in the 21st Century, Staff Study. Washington: U.S. Govt. Print. Off.: 1996.

U.S. Congress, Senate, Commerce Committee. Administration Encryption Policy. Hearings before the Commerce Committee. ___th Cong, __ sess, 19 March 1997.

U.S. Congress, Senate, Committee on Commerce, Science, and Transportation. Impact of Encryption on Law Enforcement and Public Safety. Hearings before the Committee on Commerce, Science, and Transportation. ___th Cong, __ sess, 19 March 1997. <http://www.fas.org/irp/congress/1996_hr/s960725f.htm>.

White House, Office of the Press Secretary. "Foreign Access To Remote Sensing Space Capabilities" Fact Sheet. Washington: 10 March 1994. <http://www.fas.org/irp/offdocs/pdd23-2.htm>

White House, Office of the Press Secretary. "Public Encryption Management" Fact Sheet. Washington: 16 April 1993. <http://www.fas.org/irp/offdocs/pdd5.htm>