

AIR WAR COLLEGE

AIR UNIVERSITY

STRATEGIC SURPRISE
IN AN AGE OF INFORMATION SUPERIORITY:
IS IT STILL POSSIBLE?

by

Michael D. Brice, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Grant Hammond

Maxwell Air Force Base, Alabama

Word Count: 6,415

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 2003		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Strategic Surprise In An Age of Information Superiority: Is It Still Possible?				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Michael D. /Brice				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air University Press Maxwell AFB, AL 36112-6615				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 29	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Disclaimer

The views expressed in this academic research paper are those of the author 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.

Biography

Lieutenant Colonel Michael D. Brice is a student at the Air War College, Maxwell AFB, Alabama. His experience includes past assignments as a Minuteman missile launch officer, and in command and control, combat plans, and personnel arenas. He has held assignments at the Joint, MAJCOM, Numbered Air Force, and squadron levels. His next assignment will be as the Deputy Commander, 86 Mission Support Group, Ramstein AB, Germany. His duty phone at his next assignment will be DSN (312) 480-2000. He may be reached via e-mail at Michael.Brice@ramstein.af.mil.

Contents

	<i>Page</i>
DISCLAIMER	ii
BIOGRAPHY	III
ILLUSTRATIONS	v
ABSTRACT	vi
INTRODUCTION	1
Post-Post Cold War Security Threats	6
Information Operations and Information Superiority	9
INTELLIGENCE COLLECTION	16
INTELLIGENCE, PERCEPTION, AND SURPRISE	20
CONCLUSION	27

Illustrations

	<i>Page</i>
Figure 1. Likelihood of Surprise.....	8
Figure 2. Illustrates the relationships.....	10
Figure 3. Information Hierarchy.....	21
Figure 4. OODA Loop & Information Hierarchy.....	22

Abstract

Joint Vision 2020 asserts the United States military will achieve information superiority over any future adversary. This assertion is based on three assumptions: offensive information operations will provide an accurate and complete picture of an adversary; defensive information operations will prevent adversaries from attacking friendly information systems; and the will of the US to overcome internal limitations to correctly interpret information will allow it to dominate the information realm against any opponent. However, evidence indicates these assumptions are flawed and the United States is vulnerable to strategic surprise. In fact, according to Eliot Cohen, “One might usefully call the past dozen years ‘the age of surprises.’ The US government has been surprised by the end of the Warsaw Pact, the disintegration of the Soviet Union, the Iraq invasion of Kuwait and the ensuing Persian Gulf War, the Asian Financial Crisis, the Indian and Pakistani nuclear detonations, and now the events of September 11, 2001. There is no reason to think the age of surprises is over, and there are many reasons to think we are still at its beginning.”¹

Notes

¹ Eliot Cohen, “A Tale of Two Secretaries,” *Foreign Affairs* 81, no. 3 (May-Jun 2002): 42.

Introduction

Today, the United States military faces two overriding challenges. It must find a way to provide adequate national security for the nation with a smaller force structure while simultaneously coping with a complex post-Cold War international security environment. Military leaders are confident they can meet these challenges by adopting and incorporating new advanced computer systems and global communications network technologies into all branches of the military.¹ This transformation rests upon the *assumption* that integrating new information technologies will provide the US military with *information superiority* over any adversary, at any time, across the full spectrum of conflict.²

In theory, information superiority will provide an insurmountable advantage over any adversary, allowing the US armed forces to collect, process, and disseminate an uninterrupted flow of information while exploiting and denying an adversary's ability to do the same.³ Such an advantage will provide superior knowledge to soldiers, airmen, sailors, and marines, allowing them to get inside the enemy's kill chain. Joint Vision 2020, identified information superiority as the essential element for US military transformation. By enabling a handful of new joint operational concepts—dominant maneuver, precision engagement, full-dimensional protection, and focused logistics—the US expects to obtain overwhelming advantages against any opponent.⁴ The importance of the idea of information superiority and the advantage it provides is nothing new. Sun Tzu clearly understood it centuries ago when he said, “Know the enemy and know yourself; in a hundred battles you will never know peril.”⁵

Accurate, timely, information will be a critical element of US national military power in the future. However, the assumption made in JV2020 that US forces will be able to secure information superiority against any adversary across the entire spectrum of warfare is in direct conflict with the notion that the US can be denied information superiority by a savvy and determined adversary or simply by its own inability to successfully analyze and correctly interpret the growing avalanche of raw intelligence data being collected daily.

Since information superiority is considered the relative information advantage held over an opponent, surprise can be thought of as a type of information advantage that one side obtains over another. The dictionary defines “surprise” as, “an attack made without warning or to take unawares.”⁶ A surprise attack on the US aimed at denying information superiority could be either active or passive and take several forms. For example, the infrastructure used for US collection, analysis, and dissemination of information could be targeted directly for destruction or disruption. In a similar fashion, friendly information itself could be successfully attacked by stopping, overloading, interrupting, delaying, or corrupting it. Therefore, it follows that if the US is unable to collect, interpret, or disseminate critical information in a timely manner, its military forces will be surprised. The seriousness of such an attack would depend on the level of information denial or disruption achieved by an enemy, but *any* level of surprise will invalidate the presumption of information superiority at that time. Thus, the assumption of information superiority that dominates current US military thinking will not prevent the US from being susceptible to strategic surprise in the future and, in some respects, will make it more likely and more difficult for the US to prevent.

This paper explores the vulnerability of the US to strategic surprise from an enemy attack in the information realm. Specifically, it examines vulnerabilities to US information within the operations arena and the critical role human perception plays between intelligence and surprise.

Information as a US Center Of Gravity

Information has taken on such critical importance for US economic, military, and political well being that it has been called the nation's "life blood."⁷ In fact, former Senator Robert Kerry has likened the US information infrastructure to, "a carotid artery where the nation could bleed to death if the financial system or power grid were shutdown."⁸

Embracing the new Information Age, the US has become completely dependent on the application of state-of-the-art computer and communication technologies. For example, it is estimated that over three trillion dollars in stocks, bonds, and currencies are traded on the global electronic market *daily*—or the equivalent of one and a half times the annual US budget.⁹ Also, the American military has tried to take advantage of the huge benefits that instantly available information provides. In this new age, interconnectivity and dispersed computing power have significantly increased access to and dependence upon information, making the places it resides (such as databases, programs, and networks) more attractive targets. Therefore, information itself must be protected because it can be used as a weapon or become the target of attack. As long as defensive countermeasures lag behind offensive information weapons, the US will be vulnerable to attacks that make traditional physical security measures less meaningful. Near total dependence by the US on information systems, linked to other computer systems with limited protection, presents an avenue of attack for those wishing America harm. Finally, since the cost of conducting information warfare is cheap compared to conventional warfare, many

additional actors besides traditional nation states can be expected to populate the field of possible attackers.

In *On War*, Carl von Clausewitz defined center of gravity as “the hub of all power and movement, on which everything depends.”¹⁰ With America so reliant upon information as a source of strength over all competitors, information has evolved into a center of gravity for the United States.¹¹ Although technology in the information age has greatly benefited the US, over reliance on it has the potential to make the country susceptible to great harm. British scientist C.P. Snow summed it up best when he wrote, “Technology is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other.”¹² Snow’s insight was driven home during Operation Enduring Freedom when a member of the US Special Forces was killed while trying to call in an air strike on nearby Taliban forces. Despite grave danger, his death was not caused by the enemy but because the batteries in his handheld Global Positioning System (GPS) ran out. After he replaced them and switched his GPS unit back on, the grid coordinate reading *defaulted to his own position*. Unaware of this glitch, he then passed his own coordinates to a circling US aircraft that delivered a bomb on the designated target with tragic results.¹³

Adversaries understand how information and supporting infrastructures can be used to cripple or weaken the US by attacking critical vulnerabilities of this center of gravity. Because an enemy could use proven techniques and procedures to conduct an asymmetric information attack to deny the US access to vital infrastructure and disrupt command, control, communications, and intelligence networks, the Central Intelligence Agency (CIA) “treats information warfare as one of two main threats to US national security, the other being weapons of mass destruction.”¹⁴ An information attack of any size would constitute a weapon of mass

disruption at the very least, and if it crippled infrastructure or databases irrevocably, it too would be a weapon of mass destruction. Recognizing that information has become a center of gravity for US military, political, and economic power, many futurists theorize that the US is quickly approaching a time when a terrorist or cyber warrior might be able to do more damage to the US with a keyboard than a bomb.¹⁵

Post-Post Cold War Security Threats

As the US continues to increase its reliance upon information and the systems that provide support to its economic and military leadership, it has taken up a dual-edged sword.¹⁶ On the one hand, the integration of information systems by the US offers great advantages, but on the other, it creates new and unexpected vulnerabilities.¹⁷ A recent DoD warning labeled the insecurity of the National Information Infrastructure “a tunnel of vulnerability.”¹⁸ As such, the threat of a terrorist exploiting this vulnerability to destroy or penetrate and manipulate key information systems or infrastructure could cripple or negate US attempts to dominate the information domain through information superiority.¹⁹

Globalization has been portrayed by writers in the developed Western world as a force for prosperity and peace.²⁰ However, the rest of the world takes a much different view, routinely sighting this phenomenon as the underlying cause for a decline in traditional cultural values, a weakening of the state, and a breakdown in social order.²¹ These negative aspects, both real and perceived, have been used by non-Western states and disenfranchised groups as a reason to foster intolerance and violence through religious fundamentalism, terrorism, racism, and ultra-nationalism. Because globalization is seen by these groups as benefiting some while leaving others behind, these groups often resort to terrorism to exact revenge for the perceived wrongs and injustice that globalization has inflicted upon them.²² Their willingness to attack anywhere

at anytime using increasingly destructive weapons and sophisticated techniques against civilian targets represents a new and serious threat to US security.²³

The former head of the Defense Intelligence Agency (DIA), LTG Patrick Hughes, has stated that although traditional threats from the Soviet Union have diminished, the US is now faced with a vastly more complex, diverse, and unpredictable strategic threat environment.²⁴ He believes three areas of the threat are particularly dangerous to US security: “the rise of ideologies opposed to US interests; a change in the psychology of conflict based on hatred or religion; and extreme difficulty in determining the capability, intentions, and will of an opponent.”²⁵ Furthermore, according to Secretary of Defense Rumsfeld, the overwhelming conventional capability that the US demonstrated in the Gulf War and since will probably prevent any future competitor from engaging America’s armed forces head-to-head. Instead, he believes that future competitors can be expected to challenge the US through the use of “asymmetric” means that allow them to capitalize on their strengths while trying to exploit US vulnerabilities.²⁶

When al Qaeda terrorists attacked the World Trade Center and the Pentagon the US entered into what Secretary of State Colin Powell has called, “the post-post-Cold War” world.²⁷ Prior to that event, the US felt safe and secure at home. This asymmetric attack illustrates the grave danger to the US transnational terrorists now pose and how powerful information age tools can be used to support deadly surprise attacks.²⁸ The perpetrators used global information systems and networks such as cell phones, e-mail, and the Internet for command and control and commercial airliners as guided missiles to kill over 3,000 people while striking at the heart of America’s financial and military symbols.

The transparency provided today by sophisticated intelligence collection systems provides the US with macro-level knowledge of opponents through pattern recognition. This capability allows the US to see enough of a state actor's conventional capability to make it unlikely that it will be surprised. However, because non-state actors rely on unconventional war as their method of fighting, and because US intelligence systems are not nearly as effective against this type of threat, the likelihood of surprise becomes more probable. The probability of surprise being inflicted on the US is a function of the strategic environment. In other words, the type of actor (state or non-state) and type of war (conventional or unconventional) being considered determines the likelihood. Figure 1 illustrates the relationship between these four variables and the probability of achieving strategic surprise against the US.

Figure 1. Likelihood of Surprise.

		TYPE OF WAR	
		CONVENTIONAL	UNCONVENTIONAL
TYPE OF ACTOR	STATE	<p>— —</p> <p>UNLIKELY</p>	<p>+ —</p> <p>POSSIBLE</p>
	NON-STATE	<p>— +</p> <p>POSSIBLE</p>	<p>+ +</p> <p>PROBABLE</p>

FIG. 1 LIKELIHOOD OF SURPRISE

One other important factor not represented in this matrix must be considered when trying to determine the chance of surprise. The wildcard in assessing an adversary's intentions and the

likelihood of surprise is miscalculation. In order to understand miscalculation, we must first understand perception. Perception is a human cognitive skill that is subject to both conscious and unconscious influences. Therefore, in a complex strategic environment filled with limited, ambiguous, and incomplete information, there is a high probability for misperception of the true meaning of information or events. Such misperception leads directly to miscalculation or taking a risk that the actual circumstances and situation do not warrant to a rationale actor. Based on this, the probability of miscalculation by an adversary makes the chance of the US becoming a victim of strategic surprise more likely.

Information Operations and Information Superiority

AFDD 2-5, *Information Operations*, defines information operations (IO) as “actions to affect adversary information and information systems while defending one’s own information and information systems” and divides it into two major subcategories—Information-in-Warfare (IIW) and Information Warfare (IW). IIW relates to the gain and exploit aspects of IO; IW corresponds to the attack and defend aspects of IO.²⁹

Figure 2. Illustrates the relationships.

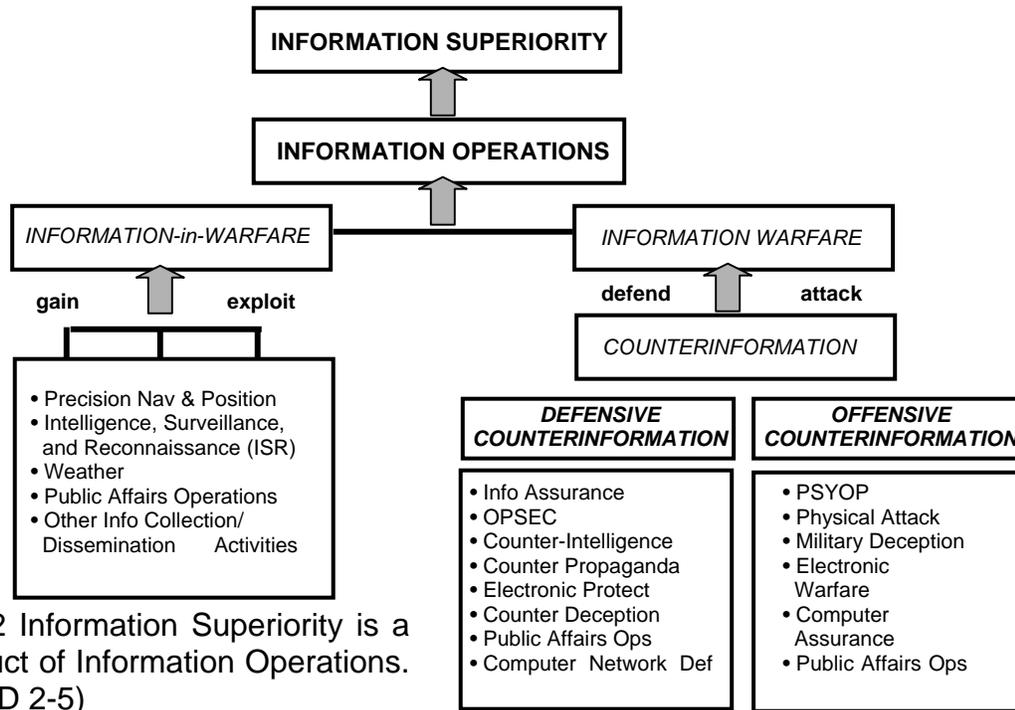


Fig. 2 Information Superiority is a product of Information Operations. (AFDD 2-5)

How IO works to produce information superiority also provides a roadmap on how an opponent can attack it, defeat it, or deny it. First, an enemy can deny the US information superiority by successfully conducting indirect or direct information warfare. Second, a failure to defend or protect friendly information can result in information superiority being lost. Third, technology might provide information transparency against an opponent, but then be wasted if military and civilian leaders fail to respond appropriately because of growing uncertainty resulting from information overload.³⁰ Such results would cripple any response to meet and defeat the threat. Because the US military has become so dependent on the receipt of timely, uninterrupted, and accurate flow of information, future asymmetric attacks will try “to disrupt, deny, degrade, destroy, or deceive US information or information systems”³¹ in an attempt to prevent the US from obtaining information superiority.

How might opponents attack US information to deny information superiority? First, all unprotected electronic equipment could be rendered useless if exposed to an electro-magnetic pulse (EMP).³² Such an EMP could be released either from the detonation of a small nuclear device in the atmosphere or from a conventional EMP generator on the ground. To understand the impact of such an attack, consider that in 1962 the US detonated a nuclear device in the atmosphere over the Pacific Ocean destroying electronic monitoring equipment nearby and seriously disrupting telephone and electric service in Hawaii over 800 miles away.³³ If an EMP were used against a major US metropolitan area like New York City, the impact could be devastating. Semiconductors used today are at least 10 million times more sensitive to damage from an EMP than vacuum tubes used in the past.³⁴ Communications systems, computer chips, the air traffic control system, financial networks, and the electric grid would be knocked out or seriously impaired. Another way to deny the US information would be to target its intelligence, surveillance, and reconnaissance (ISR) collection capability by jamming ISR platform sensors, using encryption or frequency hopping devices to transmit signals, or switching from radio and land line telephone technologies to light fiber, which does not emit any signals for ISR sensors to collect. Also in the electronic realm, simple jamming of US radio and data link communications as well as GPS -aided systems could adversely affect US military operations.³⁵

Information could also be denied to the US by introducing a virus, “logic bomb,” or some other pernicious software code into key US computer systems.³⁶ The potential effect of these and many other electronic warfare techniques could potentially render all targeted and unprotected electronic equipment useless. During the Gulf War, the US supposedly shut down Iraq’s air defense system with a virus it introduced into that country’s air defense system. If such

a technique were successfully used against the US, it could result in computer gridlock for hours, days, or weeks.³⁷

Numerous confirmed cases of successful unauthorized intrusions into US computer systems and databases exist. Such intrusions can be used to manipulate, exploit, or corrupt US information. Rogue elements within Russia are known to have successfully penetrated dozens of US military installations and industry computer networks through overseas Internet connections in an attempt to steal sensitive weapons guidance information and naval intelligence codes. Recently, hackers broke into the Air Force Research Laboratory in Rome, New York over 150 times and shut down 33 lab computer networks for several days. During this attack, the hackers copied sensitive air tasking order information with the intention of offering it for sale to the highest bidder.³⁸ The perception that only opponents of the US who possess little military power will engage in asymmetric information warfare against America would be wrong.

Such activities are not confined to individuals or fringe elements. China has placed a high priority on developing ways to destroy or neutralize US military information and infrastructures used to support high-tech weapons, intelligence sensors, and command and control functions through a new concept labeled “Unrestricted Warfare.”³⁹ A researcher at China’s Academy of Military Science observed,

if digital [i.e. digitized] forces lose the power to control information, they will not be able to stand up to mechanized forces [such as the People’s Liberation Army’s]. If they fail to acquire or transmit information, digital forces will be paralyzed, their combat capability would shrink rapidly, and they will lose the initiative on the battlefield.⁴⁰

In support of this new military thrust, China has developed cutting edge software that can allow a hacker to learn, adapt, and manipulate computer data. This type of software has already been used by China. According to RAND’s Hame Mulvenon, “the target so far has been Taiwan’s

command and control systems with the ultimate goal of hacking into US military networks that support deployments to the region.”⁴¹

An adversary can also use military deception to create a false illusion of reality that denies the US true information necessary to make a proper decision. For example, although the destructive potential of Scud missiles presented an inconsequential military threat to US and coalition forces during the Gulf War, Saddam Hussein tried to turn it into a strategic weapon by firing it on Israel in an attempt to draw that country into the war and divide the coalition.⁴² This move forced the US to redirect significant ISR and airpower assets to try to locate and destroy all Iraqi Scud missiles within range of Israel. Despite having state of the art ISR capabilities and the freedom to collect without interference from the enemy, US and coalition forces could not effectively track down and kill Iraq’s missiles during the war. Iraq was able to accomplish this surprising feat through camouflage, concealment, and deception. It skillfully employed decoys that could not be recognized as fake from 25 yards away while at the same time concealing the real missiles and transporters from coalition strike aircraft beneath low clearance highway overpasses. The effectiveness of Iraq’s deception involving Scuds is underscored by the fact that F-15Es flew over 1,400 sorties against this target set and recorded *zero* confirmed kills.⁴³

In 1998 deception was successfully used again against the US in Kosovo. There, enemy forces used decoy tanks and armored personnel carriers to great effect in reducing the attrition from allied air strikes during operation Allied Force.⁴⁴ Such deception by the enemy causes friendly forces to waste sorties and munitions on meaningless targets. It also can lead to faulty intelligence analysis on the status of enemy forces being passed to key US military and political decision makers. US leaders are dependent on accurate and timely intelligence about the enemy to properly synchronize and apply the right forces to the right targets.

Notes

¹ Air War College, Department of Leadership and Ethics Book 2, *Lifting the Fog of War*, (Air University, Maxwell AFB, Ala.: AY 2003), 220.

² *Joint Vision 2010*, (Washington, D.C.: Chairman of the Joint Chiefs of Staff), 3.

³ Jeffrey C. Horne, "Information Superiority As An American Center of Gravity: Concepts For Change In The 21st Century" (Research paper submitted to the Army War College, Carlisle Barracks, PA, 10 Apr 2000), 6.

⁴ *Joint Vision 2020*, 1

⁵ Sun Tzu, *The Art of War*, ed. and trans. Samuel B. Griffith (Oxford U.K.: Oxford University Press, 1963), 84.

⁶ *Merriam-Webster Dictionary* (New York, N.Y.: Simon & Schuster, 1974), 689.

⁷ Cohen, 42.

⁸ Robert K. Ackerkman, "Commercial Military Information Security Requirements Meld," *Signal* 50, no. 9 (May 1996): 108.

⁹ Christopher J. Rhodes, "How Real Is The Threat, And Can It Be Countered?" *Military Technology*, May 2001, 71.

¹⁰ Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 595-596.

¹¹ Horne, 1.

¹² Paul G. Kaminski, "A Problem—And An Opportunity For The AOC," *Journal of Electronic Defense*, September 1999, 55-56.

¹³ Nick Cook, et al. "Military Priorities and Future Warfare," *Jane's Defense Weekly*, 11 September 2002, 45.

¹⁴ Kevin O'Brien, "Intelligence Collection For Asymmetric Threats, Part 1," *Jane's Intelligence Review* 12, no. 10 (Oct 2000): 52.

¹⁵ ¹⁹ Alvin and Heidi Toffler, *War and Anti-War*, (New York, N.Y.: Little, Brown and Company, 1993), 151-152.

¹⁶ Cohen, 42.

¹⁷ Kevin J. Kennedy, Bruce M. Lawlor, and Arne J. Nelson, *Grand Strategy for Information Age National Security, Information Assurance for the Twenty-First Century*, (Maxwell AFB, AL: Air University Press, August 1997), vii.

¹⁸ O'Brien, 52.

¹⁹ John T. Chenery, "Transnational Threats 101: Today's Asymmetric Battlefield," *Military Intelligence* 25, no. 3 (Jul-Sep 1999): 5.

²⁰ Jan Scholte, *What is Happening?* (Cambridge, M.A.: St. Martin's Press, 2000), 55.

²¹ *Ibid.*

²² Stanley, Hoffman, "Clash of Globalizations," *Foreign Affairs* 81, no. 4 (Jul/Aug 2002): 107.

²³ Scholte, 10.

²⁴ Horne, 1.

²⁵ *Ibid.*

²⁶ Rumsfeld, 25.

²⁷ Richard N. Haass, "The 2002 Arthur Ross Lecture to the "Foreign Policy Association," 22 April 2002.

²⁸ *Ibid.*

Notes

²⁹ Ibid.

³⁰ Michael I. Handel, *War, Strategy and Intelligence*, (Totowa, N.J.: Frank Cass & Co. Ltd., 1989), 21.

³¹ Michael E. O'Hanlon, *Technological Change and the Future of Warfare*, (Washington, D.C: Brookings Institute, 2000), 58.

³² Ibid.

³³ "Crash Your Office Without Touching A Keyboard," n. p. On-line. Internet, 6 February 2003, 3. Available from <http://www.cs.dartmouth.edu/~cs7/papers/bradford-p2.html>.

³⁴ O'Hanlon, 58-59.

³⁵ Ibid, 58.

³⁶ Rhodes, 72

³⁷ "Information Warfare," n. p. On-line. Internet, 6 February 2003, Available from <http://netsecurity.about.com/library/weekly/aa011199.htm>.

³⁸ Horne, 7-8.

³⁹ Qiao Liang and Xiangsui Wang, "Unrestricted Warfare," In FBIS [Foreign Broadcast Information Service], 1999.

⁴⁰ Air War College, Department of Warfighting, Future Warfighting Environments Unit 2, *Patterns in China's Use of Force: Evidence From History and Doctrinal Writings*. Air University, Maxwell AFB, Ala.: AY 2003. 110.

⁴¹ Horne, 8.

⁴² Benjamin S. Lambeth, *The Transformation of American Air Power*, (Ithaca, NY: Cornell University Press, 2000), 145.

⁴³ Ibid.

⁴⁴ Timothy L. Thomas. "Kosovo And The Current Myth Of Information Superiority." *Parameters* 30, no. 1 (Spring 2000): 16.

Intelligence Collection

All information operations are important to achieving information superiority, but intelligence is especially important and must be considered first among equals.¹ In the future, the quest to achieve information superiority and avoid surprise will depend on the ability of US forces to be supplied with timely and accurate intelligence on the enemy and the potential operational environment.² As opponents adopt new information technologies to support their own offensive and defensive information operations, such technologies make US monitoring of potential threats significantly more challenging. Because “information systems” do not necessarily manifest themselves in the form of physical things (like ships, planes, and tanks), US Cold War-era intelligence collection platforms are currently not able to monitor opponent information system development, testing, and deployment in a meaningful way.³ Furthermore, no intelligence organization can prevent surprise from a known or unknown actor if it does not understand that the threat exists. Without a perceived threat, the intelligence collection process cannot be efficiently and accurately applied. During the Scientific Advisory Board debrief on Predictive Battlespace Awareness, “98 percent of collected intelligence data ends up on the cutting room floor.”⁴ The report goes on to state, “existing ISR data often ends up on the floor because of the lack of someone who cares about the data (or knows they should care).”⁵ Despite spending a combined \$12.6 billion annually on classified imagery, a lack of coordination and duplication of effort while neglecting other areas led to a failure on the part of the US intelligence community to provide any advanced warning of the nuclear tests conducted by India in 1998.⁶ As a result, this test took the US by complete surprise.

Unfortunately, today US intelligence agencies are not well suited to anticipate, analyze, and investigate asymmetric threats that now pose the greatest danger to US national security.⁷ The magnitude of the challenge facing US intelligence agencies to ferret out individuals or organizations planning to attack the United States and therefore prevent surprise is clear when one considers that a cyber-attack on information or supporting infrastructure can be originated from almost any one of 100 million computers now connected to the Internet.⁸ When such wide access is combined with the knowledge that US commercial systems largely operate without built-in security measures, the potential threat of a digital Pearl Harbor attack is frighteningly real to the intelligence community.⁹

In order to prevent future surprise, the US intelligence community must move away from its almost total reliance on space-based sensors as the primary means to collect data.¹⁰ After the terrorist attacks on September 11, 2001, senior officials requested funds beyond the \$10 billion spent annually on counter-terrorism to increase human intelligence (HUMINT) capabilities.¹¹ But HUMINT intelligence has its own drawbacks. To guard against a double cross, the reliability of incoming HUMINT intelligence must always be crosschecked by other means, and the source must continuously be vetted for loyalty and reliability.

Even though HUMINT offers the best method to determine the intentions and actions of enemies to the US, such as terrorists who rely on asymmetric attack, no intelligence source can address the “weakest link” in computer security. According to computer hacker Kevin Mitnick, “the government’s best efforts to stem the rising tide of computer crime will be largely ineffective unless those efforts address the human failures that make most computer intrusions possible...money spent on assessing computer vulnerabilities and security measures is wasted because none of them address the weakest link in the computer security chain.”¹²

Human failings that compromise computer and information security can be divided into two categories—innocent mistakes and criminal conduct. Innocent mistakes take the form of unintended system compromise through unintended password compromise or system access. On the other hand, there have always been individuals willing to betray the US and compromise vital information for money or because of misplaced loyalty. One of the best known cases involves John Walker, who worked as a Soviet spy for over 18 years. During that time he sold secrets that compromised naval intelligence codes, code machines, and classified documents.¹³ A more recent case concerns former CIA agent Aldrich Ames. The damage he inflicted during nine years of spying was not limited to the thousands of pages of classified documents he turned over to the Soviets. The treachery in this case took a high toll in blood when Ames' betrayal led to the arrest and execution of 10 Soviet officials for spying on behalf of the US against the Soviet Union.¹⁴ However, not all spies are motivated by money. Jonathan Pollard, a US Navy intelligence analyst, was led to spy on behalf of Israel because of his religion and uncontrollable desire to assist that country by whatever method possible. Pollard used his access to classified intelligence libraries to freely pass over 1,000 classified documents to Israeli intelligence handlers.¹⁵ Today the intelligence community relies on efficient sources that allow greater protection and ease of access at the cost of more inclusive forms of intelligence that provide greater security.¹⁶ As long as the US continues to pursue intelligence methods and means that do not adequately address threats across the spectrum, it will remain vulnerable to a surprise attack.

Notes

¹ John Barnett, "Grasping Joint Vision 2010," *Joint Force Quarterly*, no. 17 (June 1996): 30.

² Alan D. Campen and Douglas H. Heath, *Cyberwar 3.0*, (Fairfax, Virginia: Armed Forces and Electronics Association International Press, 2000), 104.

³ *Ibid.*

Notes

⁴ *Air Force Scientific Advisory Board Report on Predictive Battlespace Awareness to Improve Military Effectiveness—Volume 1: Summary*. Draft Report, (Washington, D.C., June 2002) 52.

⁵ Ibid.

⁶ Kevin O'Brien, "Intelligence Collection For Asymmetric Threats, Part 2," *Jane's Intelligence Review* 12, no. 11 (Nov 2000): 51.

⁷ Christopher F. Chyba, "Toward Biological Security." *Foreign Affairs*, May/June 2002, 123.

⁸ Ibid, 125.

⁹ "Jolting Destruction Galvanizes U.S. Agencies To Walk The Walk," *Signal* 56, no. 3 (Nov 2001): 22.

¹⁰ Lambeth, 13.

¹¹ Kevin O'Brien, "Carnivore Feeds On PATRIOT," *Jane's Intelligence Review* 13, no 12 (December 2001): 53.

¹² Ibid.

¹³ *Walker was "Intrinsically Evil,"* On-line. Internet, 6 February 2003. Available from <http://rf-web.tamu.edu/security/SECGUIDE/spystory/walker.htm>.

¹⁴ *Ames: Too Many Weaknesses,* On-line. Internet, 6 February 2003. Available from <http://rf-web.tamu.edu/security/SECGUIDE/spystory/ames.htm.htm#aldrich%20amis>.

¹⁵ *Pollard: Grandiose Imagination,* On-line. Internet, 6 February 2003. Available from <http://rf-web.tamu.edu/security/SECGUIDE/spystory/pollard.htm#jonathan%20>

Jay%20pollard.

¹⁶ O'Brien, 54.

Intelligence, Perception, and Surprise

According to John Boyd, the father of the Observation-Orientation-Decision-Action (OODA loop), the fundamental key to victory in war is human perception. Boyd believed perception was key because *only humans fight wars*. Other factors such as circumstances, terrain, and weapons were less important. Because the OODA loop offers a comprehensive and simple methodology for operating at a faster tempo than the enemy, it makes US actions appear to be ambiguous (unpredictable) to the enemy, causing confusion and disorder in their response. Therefore, Boyd believed that getting “inside the mind of the enemy” and beating him to the next move by operating at a faster tempo is where battles are won. Today the OODA loop is employed throughout the US military and, when supported with accurate and timely intelligence, provides a crucial military advantage.¹

Intelligence plays a vital role in every level of successful military operations and is especially important for allowing the US to operate inside an enemy’s decision cycle. Proper employment of collection and analysis assets is essential for commanders to gain and maintain information superiority. Without accurate intelligence, US forces will lose essential advantages of surprise, operational security, and flexibility. It is the function of intelligence to collect data and provide information to decision makers. Joint Publication 1-02 defines intelligence as:

- (1) The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.
- (2) Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.²

Thus, information is the essential product from which all intelligence supporting information superiority flows.

But what is information? A generally accepted information hierarchy (Figure 3) illustrates distinct levels of “information.” At the bottom are data--observable raw facts. "Information," derived from data, consists of the trends or patterns that emerge from quantities of perceived data.³ The third layer, “knowledge,” represents attempts to discern the truth through reasoning. "Wisdom" results from gaining insight from knowledge.⁴ Finally, there is “truth,” an accurate understanding of reality and the meaning of information. Truth is where perception and reality are one in the same or in agreement.

Figure 3. Information Hierarchy.

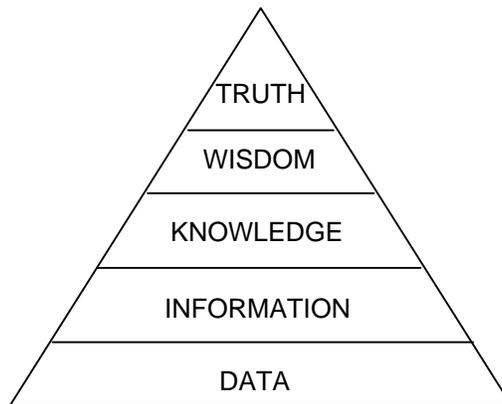


FIG. 3 INFORMATION HIERARCHY

These five levels of the information hierarchy relate to the OODA decision-making cycle. First, Observation acquires data. Next, Orientation converts the data into information. Then, Decide converts information into orders. And finally, Act converts orders into action. The process is a loop because as you act, you observe the results and start the process all over again.⁵ See Figure 4.

Figure 4. OODA Loop & Information Hierarchy

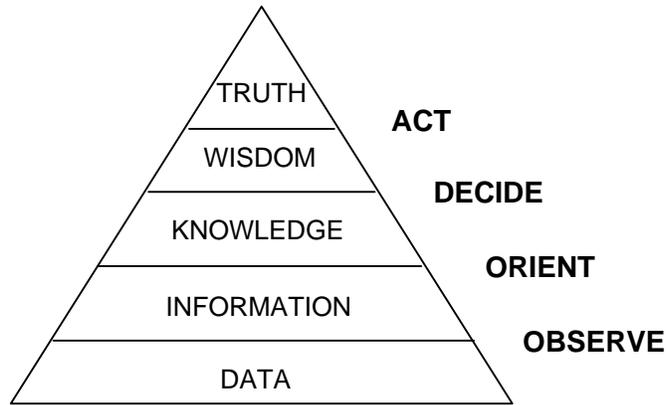


FIG. 4. OODA LOOP & INFORMATION HIERARCHY

However, information in the context of military intelligence may not accurately describe reality for three reasons. First, information used for intelligence purposes can be manipulated or distorted by an adversary. Second, information derived from intelligence is a product of human perception and therefore subjective in nature, making it subject to bias or/and misreading of the true meaning. Third, relevant signals (desired information) do not exist in a vacuum. Signals can be overlooked because of their ambiguous nature or simply become lost in an overwhelming cascade of noise (irrelevant information) that is collected in the intelligence process.⁶ No matter what the reason, corruption, misperception, or missed signals, bad or very limited information inevitably taints the levels above them in the information hierarchy and negatively impacts the OODA decision-making cycle. Therefore, protection of information becomes critical to the integrity of knowledge, wisdom, truth, and to the accuracy and appropriateness of decision-making that lies at the heart of vulnerability to surprise.

The damage that can be done when a leader bases decisions upon corrupted information or misinterprets accurate information cannot be overstated. Hitler's response to the Allied invasion of Europe in World War II offers a perfect example. Incredibly, for weeks after the Allies landed at Normandy on D-Day and subsequently pushed twelve divisions ashore, Hitler

remained convinced that the “main Allied invasion force” would strike at anytime further north on the French coast at Pas-de-Calais. For this reason, he rebuffed all pleas from his field commanders to release the Panzer forces situated around Calais so they could take part in a counterattack on the Allied forces at Normandy. Why did Hitler fail to respond appropriately to the invasion? First, he was the victim of a successful Allied deception campaign, “Operation Fortitude,” that planted information indicating that Pas-de-Calais would be the sight of the main Allied invasion. Second, this deception effort reinforced what Hitler wanted to believe. Because the Pas-de-Calais area offered the shortest distance across the English Channel for the Allies, it made the most sense from a logistics and lines of communications standpoint. Thus, when the D-Day landings occurred, Hitler failed to make timely decisions, thereby missing the opportunity to annihilate the invaders while their backs were to the sea.⁷

The 1991 Gulf War offers two more examples of how false perceptions can result in surprise. Before the Al Firdos bunker in downtown Baghdad was destroyed by F-117s, US intelligence knew that the facility was constructed as an air-raid shelter for the general population. However, Iraqi attempts to camouflage the roof, the proximity of its location to Iraqi intelligence headquarters, and radio emissions from the site led American intelligence analysts to conclude the facility was an important command and control center worthy of attack, regardless of the chances of noncombatants being killed.⁸ The loss of over 100 women and children was a public relations disaster for the US.⁹ As a result, this single event accomplished what Iraqi air defenses had not been able to—cause US leaders to call an immediate halt to further air raids on downtown Baghdad. After the war it was determined this shelter might have been a hideout for senior Iraqi officials, but it had minimal radio equipment and was not serving as an important command and control facility.¹⁰ The intelligence “failure” in this case resulted in a false

perception, which in turn led to surprise for the US when a large number of noncombatants were killed.

Finally, the devastating attack by US airpower on Iraqi forces retreating from Kuwait in hundreds of stolen civilian vehicles along a two-mile stretch of road that became known as the “Highway of Death” offers another example. After the battle, video footage and accompanying press accounts portrayed a scene where hundreds of Iraqi armored vehicles and thousands of lives were lost, and thus, the victimizer became the victim.¹¹ In fact, US intelligence analysis after the battle revealed a much different reality. Although over 1,000 civilian vehicles had been destroyed in the attack, only 28 militarily meaningful armored vehicles and 200-300 Iraqi soldiers had actually been killed. But because the news networks’ version of events went unchallenged, the perception that American forces conducting a “turkey shoot” against a defenseless enemy stuck. This misperception then became an important factor in President Bush’s decision to end the war after only 100 hours of the ground campaign. His decision allowed the Republican Guard to escape destruction. Those same enemy armored units were later instrumental in suppressing the Shiite and Kurdish uprisings inside Iraq after the war trying to overthrow Saddam Hussein in 1991.¹²

Another important factor relating to information, perception, intention, and truth is the element of time. Effective intelligence is expected to produce accurate and timely information. However, the information collected by reconnaissance and surveillance may or may not be true or “good” (accurately representing reality) at any given time. For example, US reconnaissance flights over the desert in western Iraq during the Gulf War did not find Scud missiles because (1) they were not there at all; (2) successful enemy deception operations concealed them from sensors; or (3) the Scuds were moved into the area in between reconnaissance missions. In all

three cases, US intelligence analysis would produce the same assessment—that no Scuds were located in the sector being looked at. In the first case this perception would coincide with the truth and be correct. However, in the second and third cases perception based on discrete available intelligence information would not be true. From the second and third cases, we can see how the timing of intelligence collection could provide leaders with a false perception of the situation and lead to surprise when they discovered the actual reality.

Obviously, many factors can cloud accurate human perception of reality—cultural bias, language differences, national historical experiences, wishful thinking, projection of one’s own experiences, timing, opponents’ doctrines or capabilities, and political influences.¹³ Michael Handel discusses the disconnect between intelligence and perception:

Intelligence is supposed to make subjective perception closer to the ‘objective reality,’ but even the best intelligence organization in the world can never guarantee an accurate perception of the opponent nor the acceptance of its analysis. Strategic analysis mistakenly assumes that our perception of the opponent is usually accurate, which makes the design and selection of a rational strategy possible. The US vs Vietnam; Israel vs Arabs; Arabs vs Israel; Allied overestimation of the success of strategic bombing; and Japan’s conception of the US reaction to the attack on Pearl Harbor all illustrate the extent of the gap between reality and perception and how this unavoidable gap sharply reduces choosing a rational strategy.¹⁴

The fact that humans are naturally unable to view their environment objectively and prone to incorrectly perceiving the meaning of data, along with the increased vulnerability of intelligence data and information to be distorted by adversaries, increases the likelihood of enemies inflicting strategic surprise upon the US.

Notes

¹ Grant T. Hammond, *The Mind of War*, (Washington D.C.: Smithsonian Institution Press, 2001), 122-123.

² Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, (Washington, D.C., 12 April 2001), 208.

Notes

³ Chairman Joint Chiefs of Staff, *Concept For Future Joint Operations—Expanding Joint Vision 2010*, (Fort Monroe, Virginia: May 1997), 2.

⁴ Robert J. Bunker, *Information Operations and the Conduct of Land Warfare*. Arlington, Virginia, The Institute of Land Warfare Association of the U.S. Army, Land Warfare Paper No. 31, (October 1998), 5.

⁵ Hammond, 4-5.

⁶ Roberta Wohlstetter, *Pearl Harbor: Warning and Decision*, (Stanford, CA: Stanford University Press, 1962), 691.

⁷ Brown, 705-706.

⁸ Michael R. Gordon and Bernard E. Trainor, *The General's War*, (New York, NY: Little, Brown and Company. 1995), 324.

⁹ Lambeth, 144.

¹⁰ Gordon, 326.

¹¹ *Ibid*, 370.

¹² U.S. News & World Report, *Triumph Without Victory*, (New York, N.Y.: Times Books, 1992), 310.

¹³ Handel, 17.

¹⁴ *Ibid*.

Conclusion

The fact that the United States is reliant upon the free and uninterrupted flow of accurate, timely, and complete information as a fundamental source of political, economic, cultural, and military dominance is irrefutable. Today information has become so important to the health of the nation that it has joined only a handful of other key concepts and ideas as a center of gravity around which all else revolves. Because current and future enemies cannot hope to match America's nuclear or conventional military capabilities, adversaries can be expected to attack perceived weaknesses of the US in the information domain through asymmetric warfare. Such attacks will attempt to pit their strengths against US weakness. Today virtually any actor from nation states to terrorist groups to individual hackers, can threaten US national security. Each can target and carry out potentially devastating attacks on US information and supporting infrastructure in an attempt to deny the US the essential enabler for its 21st century defense plans—information superiority. Thus, each could bring America's military to its knees by denying it an indispensable source of its overwhelming advantage.

To understand how the loss of information superiority can precipitate strategic surprise, one must appreciate the unique relationship between information and intelligence. Intelligence collection is the means of gathering data that is the basis for acquiring knowledge. In turn, this knowledge is used as a basis for providing military and civilian leaders with intelligence assessments about an area of interest or perceived threat. Such intelligence assessments are then used as a window into the strategic threat environment that channels and focuses the perception of leaders about the real nature of a threat or the true intentions of an opponent. These perceptions about the security landscape are then used to guide political and military leaders

while they try to make prudent decisions that optimize friendly military operations to defend the nation. In the context of military security, information and intelligence are so closely related they cannot be separated. However, information is unique because it possesses a qualitative and quantitative nature that influences the entire decision making process. Either of these two qualities can negatively influence the value and correctness of intelligence assessments, which in turn, can lead to false perceptions by leaders about a given situation, circumstance, or event. Because perception—the key to how leaders view the world—is based on correct information supplied by intelligence, misperception of reality is based on incorrect information supplied by the intelligence process. Misperception then can be expected to degrade the appropriateness of a leader's decisions.

The historical examples in this paper highlight that US information *is* vulnerable to attack. Because the US is vulnerable to information warfare and information corruption, opponents can successfully influence and manage the perception of US leaders, meaning they can also achieve strategic surprise. Carried to a logical conclusion, the fact that the US has been shown to be vulnerable to surprise negates the presumption in current military doctrine that the US will achieve and hold information superiority over any opponent across the entire spectrum of warfare. This aspect of current US military thinking is clearly false.

As the civilian and military masters of the US armed forces continue to trumpet the benefits and advantages of transformation, they would do well to reconsider that information superiority has definite limitations. They must never forget that although information superiority by US forces may be present at any one time, such a state is only a relative advantage and not an absolute condition that will exist for all time. Only by fully appreciating this important point can American military leaders take the appropriate steps necessary to adequately man, train, and

equip the armed forces. Adequate preparations must account for the certain reality that in the decades ahead, on some far flung battlefield, the desired US goal of information superiority will give way to information parity or even something less—which then becomes the norm.

There is no doubt that new Information Age technologies are transforming the US military by supplying information of previously unimaginable quantity, quality, and accuracy. Information of such “richness” can be used as a super lubricant to make everything work smoother, faster, and better. However, the US military must guard against the illusion that uncertainty on the battlefield now only applies to the enemy. As long as offensive information warfare technologies continue to lead information security measures and safeguards, the US will remain highly vulnerable to strategic surprise. Since the likelihood of surprise in the future is almost assured, the best defense against a sudden attack is not trying to reduce the probability of such an event happening, but to develop plans, doctrine, and strategies now to limit the extent of the damage when it occurs. Only then can the US feel secure in the knowledge that it is better prepared at every level than the enemy—whoever that may be.