Information Operations as a Counter to US Air Dominance: A Rival's Perspective

A Monograph

by

Major David A Harris, Jr.

USAF

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

AY 06-07

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
02-05-2007	AMSP Monograph	July 2006 - May 2007

4. TITLE AND SUBTITLE
Information Operations as a Counter to US Air Dominance: A Rival's Perspective

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major David A. Harris, Jr. (USAF)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Advanced Military Studies Program
250 Gibbon Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Command and General Staff College
1 Reynolds Avenue
Fort Leavenworth, KS 66027

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this monograph is to answer the question of what lessons over the past ten years of US air operations have foreign militaries integrated into their doctrine and organizations to counter US air dominance. By examining the air campaigns in Kosovo, Afghanistan, and Iraq through the lens of Chinese and Russians analysts, information operations has been the key lesson learned to counter US air dominance. From this analysis, some broader conclusions were made concerning the conduct of IO in peace-time, the confusion surrounding IO terminology, the challenges of identifying deception in the targeting and operational analysis process, and the integration of IO and air superiority objectives within a campaign.

15. SUBJECT TERMS
Foreign Lessons Learned, Information Operations, Kosovo, Afghanistan, Iraq, Air Power, and Deception.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kevin C.M. Benson, COL, US Army
UNCLASS	UNCLASS	UNCLASS	UNLIMITED	62	19b. TELEPHONE NUMBER *(include area code)* 913-758-3302

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major David A. Harris, Jr.

Information Operations as a Counter to US Air Dominance:

Approved by:

_____ Monograph Director
Darric M Knight, LTC, USMC

_____ Director,
Kevin C.M. Benson, COL, AR School of Advanced Military Studies

_____ Director,
Robert F. Baumann, Ph.D. Graduate Degree Programs

Abstract

Information Operations as a Counter to US Air Dominance by Major David A. Harris, Jr., USAF, 62 pages.

The purpose of this monograph is to answer the question of what lessons over the past ten years of US air operations have foreign militaries integrated into their doctrine and organization to counter US air dominance. By examining the air campaigns in Kosovo, Afghanistan and Iraq through the lens of Chinese and Russian analysts, information operations has been the key lesson learned to counter US air dominance. From this analysis, some broader conclusions were made concerning the conduct of IO in peace-time, the confusion surrounding IO terminology, the challenges of identifying deception in the targeting and operational analysis process, and the integration of IO and air superiority objectives within a campaign.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

Ensuring a competitive advantage through military power and strategy remains a critical element of the national security equation. Often times, the threat of force is enough to deter an adversary from their goals. Unfortunately, when this form of deterrence fails some degree of military action must back up the threat. John Gaddis argues that the most effective way to implement military action, as well as achieve a degree of surprise is asymmetrically, or applying your strengths against an enemy's weakness.[1] This strategy is not new.

The great military strategist Sun-Tzu wrote about avoiding the enemy's strengths and striking his weakness when he least expects an attack. For a strategy that is so well known and practiced, how does a nation exploit this concept and expect to be decisive in war? One way to exploit this strategy is to collect intelligence by examining an adversary at war and identifying their strengths and weaknesses. Using this information, a nation can change their military by developing asymmetric capabilities. Based on that premise, this monograph will answer the question of what lessons, over the past ten years of United States (US) air operations, have foreign militaries integrated into their doctrine and organization to counter US air dominance. From research, one lesson stands out above the rest. Information operations (IO) have become the key asymmetric capability which has transformed foreign military doctrine and organizations to counter US air dominance.

Colonel John Warden, air power theorist, understood the evolving nature of information operations. While he did not specifically define IO, he stated "information will become a prominent, if not predominant, part of war to the extent that whole wars may well revolve around

[1] John Gaddis. "National Security: On Strategic Surprise", *Hoover Digest*. Spring 2002. Downloaded from http://www.hooverdigest.org/022/gaddis.html

seizing or manipulating the enemy's data sphere."[2] Since Colonel Warden's prediction in 1995, advances in information technology have created many different definitions of IO. This monograph will use the Air Force definition of IO since this study examines the air campaigns over the past ten years and focuses on how adversaries use IO as a counter to US air dominance. Air Force Doctrine Document 2-5 defines IO as the "integrated capabilities of influence operations, electronic warfare, and network warfare operations along with integrated control enablers (ICE) to influence, disrupt, corrupt, or usurp adversarial human or automated decision making."[3] Influence operations are military capabilities used to affect the perceptions and behaviors of leaders, decision-makers, and people. Influence operations include psychological operations, military deception, operational security, counterintelligence, and public affairs. This definition of IO not only differs from joint doctrine but also from other country's definitions of IO due to slightly different interpretations of past events. Therefore, it is history and a country's subjective interpretation of events, that provides the data for understanding why each country chose the lessons they did.

From a historical perspective, this monograph examines the US air campaigns in Kosovo, Afghanistan, and Iraq. These three air campaigns outlined in chapter two not only supply the historical context for understanding what lessons other countries identified but also reinforce the fact that IO has become an indispensable part of US air superiority. The methodology for examining these air campaigns consists of understanding the objectives, analyzing the effectiveness of IO within the air campaign, and US lessons learned. Often times, the lessons the US draws from an operation may not be the same lessons identified by other countries because of

[2] Colonel John A. Warden III, "Air Theory for the Twenty-first Century", Aerospace Power Chronicles, "Battlefield of the Future: 21st Century Warfare Issues", 1995.

[3] Air Force Doctrine Document 2-5, "Information Operations". p. 1. 11 January 2005.

conflicting interpretations of historic events. So what value is history when its lessons are often contradictory in nature?

John Gaddis warns that studying the past does not guarantee future success but provides a context for understanding what worked and what did not in a situation and provides the database from which theories are derived.[4] Knowing this, foreign militaries can use history to look for operational patterns to template their adversary's actions. Since countries may identify different lessons based on their interpretation of a given situation, it is important to analyze more than one event to find a trend or identify a key lesson over time. Selecting specific countries to analyze the three air campaigns as a comparative analysis, now becomes essential for developing the argument that IO has become the key lesson learned to counter US air dominance.

Chapters three and four of this study focus on the lessons observed by Chinese and Russian analysts. The main factors for selecting China and Russia centered on their potential ability to threaten US national security, the capabilities of their air force, and the maturity of their aviation industry. While the 2002 US National Security Strategy (NSS) highlighted China and Russia as "great powers in the midst of internal transition"[5], the 2006 NSS praises China and Russia for their economic reforms but warns of their "military expansion in a non-transparent way."[6] Instead of expanding their militaries, China and Russia opted to selectively modernize critical capabilities. Not only have China and Russia modernized their air force but they have also increased their emphasis on IO as a key asymmetric capability to counter US air dominance.

China and Russia's emphasis on IO has restructured aspects of their military doctrine and organization. The methodology to show how IO changed each country's doctrine and organization requires analysis in four areas. First, this paper examines how each country views

---

[4] John Gaddis. (2002). *The Landscape of History*. New York: Oxford University Press. p. 10
[5] Ibid, p. 26
[6] United States National Security Strategy 2006. [electronic version: http://www.whitehouse.gov/nsc/nss/2006/nss2006.pdf] p. 41

asymmetry and information operations as compared to the US. Next, this monograph will show that China and Russia clearly identify information operations as a key lesson learned from the past ten years of US air operations. Understanding both China's and Russia's definitions forms a baseline from which a comparative analysis will follow. Once concepts are defined, an analysis of each country's military doctrine will show how IO has changed their doctrine. The same analysis that showed how IO influenced military doctrine must also show how it changed their organization. Finally, chapter five summarizes the conclusions of this study.

The following chapter outlines the major air campaigns over the past ten years and shows the importance of gaining air superiority in any type of war. According to Air Force Doctrine Document 2-5, IO is an integral part of air superiority. The document states that:

> "While electronic warfare (EW) operations have long been integrated into counter-air operations, there are other capabilities of IO that can be used. Network warfare operations can provide spurious, false, and/or misleading information to enemy defensive operations. Influence operations have also been used extensively to achieve air superiority."[7]

Since the information domain crosses all other mediums, it is necessary to gain information superiority over the adversary as well as air superiority. Air defense networks were designed to counter or delay an adversary's ability to gain air superiority and these networks require detailed information to find, fix, target, and track enemy aircraft. Air defense networks gain information through electronic emissions and distributed communication networks. As such, IO is capable of disrupting both of these spheres. More importantly, adversaries now recognize the value of not only securing their air defense networks but using IO to confuse or deceive enemy air strikes.

[7] Air Force Doctrine Document 2-5, "Information Operations". p. 7. 11 January 2005

CHAPTER TWO

US AIR OPERATIONS

Kosovo and Operation Allied Force (OAF)

The air campaign in Kosovo and Serbia in 1999 marked a turning point for air power. The air-dominant strategy used by the North Atlantic Treaty Organization (NATO) proved that air power alone was now viewed as a capable means for achieving political objectives. Even though critics may argue whether or not air power alone prompted Milosevic to accept the interim political settlement negotiated at Rambouillet, there is no doubt that air power *set the necessary conditions* to compel the Serbian leader. To that end, NATO's strategy hinged on one key, friendly objective that the component commanders struggled hardest to maintain and that was to protect the coalition's center of gravity—maintaining the unity of the coalition.[8] IO played a critical part in maintaining that unity.

At the strategic level, the alliance effectively employed IO through the use of psychological operations, public affairs, and counter-propaganda to maintain the unity of the coalition. The value of IO to shape outcomes was recognized at the strategic level however, it was lost at the operational and tactical levels. At the operation level, strict information assurance measures removed the allies from knowing the specifics of US F-117 and B-2 sorties however, operational security (influence operations) violations were discovered concerning the NATO air tasking order sorties. Tactically, the alliance was hampered by the coalition targeting process and stove-piped battle-damage assessments which resulted in striking many false targets (deception) effectively prolonging the air war and NATO from achieving its goals.

[8] Benjamin Lambeth (2001). *NATO's Air War for Kosovo; A Strategic and Operational Assessment.* Rand Project AIR FORCE: Santa Monica. p. 12.

NATO's goals were to demonstrate resolve against Belgrade's repressive measures against the Albanian population in Kosovo, deter Milosevic from continuing the ethnic cleansing, and damage Serbia's capacity to wage war against Kosovar Albanians in the future or spread the war to neighbors by degrading Serbia's military capacity.[9] While the ends were clear, the ways of achieving those goals were not. This created challenges for air planners to develop new air strategies, objectives, and targeting methodologies that were compatible with coalition air warfare while still achieving the military and political end state.

Both US and NATO leaders believed that high, friendly casualty rates were a critical vulnerability and the greatest threat to maintaining the NATO alliance. As such, they were reliant on IO's integrated control enablers [10] like Intelligence Surveillance and Reconnaissance (ISR) and predictive battle-space awareness[11] because they believed that would provide them greater information about the enemy and more precision strike capability to minimize collateral damage with a smaller force. While some critics believe that every effort was made to minimize the size of the force for this operation,[12] senior military leaders contend that the size of the operation stemmed from the assumption that the bombing was only supposed to last three nights.[13] Given the success of air power in Desert Storm and the belief that "advances in technology have led to a widespread expectation that military operations could be conducted with few or no casualties on

[9] As cited from the Unclassified Report to Congress. Kosovo: Operation Allied Force After-Action Report. 31 Jan 2000, downloaded from website in October 2006. [electronic document] http://www.defenselink.mil/pubs/kaar02072000.pdf

[10] Air Force Doctrinal Document 2-5, Information Operations, defines integrated control enablers (ICE) as separate and distinct capabilities that when integrated, produce effects greater than any single capability. ICE, formerly information-in-warfare includes ISR, network operations, predictive battlespace awareness, and precision navigation

[11] Predictive Battle-space Awareness is defined by AFDD 2-5 as knowledge of the operational environment that allows the commander and staff to correctly anticipate future conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions.

[12] Charlie Lyon, Operation Allied Force: A lesson on Strategy, Risk, and Tactical Execution. Comparative Strategy, 2001. p. 59.

[13] Phone conversation with Lt Gen (retired) Short citing that the operation started small because the air campaign was supposed to last only 3 nights—he recalls no restrictions placed on the overall size of the operation.

either side,"[14] both NATO and the US looked to air power as the means and IO as one of the ways to resolve the crisis.

The US plan called for overwhelming air power aimed at the regime in Belgrade and not at the population.[15] NATO's plan exclusively used air power as the means and gradual escalation of air strikes along with IO as the ways for achieving a negotiated settlement with Milosevic. Had both plans synchronized IO at all levels and agreed on the necessary targets then the air strikes as a form of coercion would have had a much greater psychological impact earlier in the air war. Contrary to the argument posed by Robert Pape over the effectiveness of air strikes as a form of coercion[16], gradual escalation could coerce a belligerent leader using the appropriate axiological[17] or influence targets and achieving the desired psychological effects. This type of axiological or "value targeting" relies on integrated control enablers such as ISR to accurately target those nodes that Milosevic believes most important to him. Essentially, IO themes, psychological operations, and offensive air operations (air strikes) must all focus on the enemy's center of gravity.

If the IO campaign had more cohesion at the operational and tactical level, the bombing campaign may well have ended before June 9, 1999. The amount of time that the air campaign took to compel Milosevic to sign the interim settlement allowed Belgrade to develop an asymmetric strategy to delay the effects of the coalition's air war until the Serbian military could

---

[14] N. T. Jefferson, "Battlefield Exploitation". Department of Land Warfare on behalf of Joint Doctrine and Concepts Centre (Shrivenham, UK), dated 5 Nov 2000.

[15] As cited by a 24 April 1999 NATO statement. Accessed from website on October 2006. http://www.basicint.org/europe/NATO/99summit/10-13.htm

[16] Robert Pape argues that airpower, as a form of coercion, has significant drawbacks because coercion involves the destruction of certain target sets and does not require the complete annihilation of targets to nullify his means of resistance.

[17] Axiological targeting is the use air, space, and information power to force a behavior shift in belligerent leadership in the quickest and most economical ways possible. Axiological targeting sees nonmilitary centers of gravity as more strategic and counter-value targets as more important than counterforce targets. Cited from "What Should We Bomb" by Dr. Paul Kan and accessed in January 2007. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj04/spr04/kan.html

eliminate the Kosovo Liberation Army and continue their ethnic cleansing. Essentially, Milosevic "tried at least three strategies for imposing costs on NATO: creating casualties (psychological operations); fostering sympathy through its own suffering (deception and psychological operations); and disrupting NATO cohesion."[18] Overall, these strategies had little success and NATO prevailed. Air power along with IO at the strategic level, had produced two strategic effects that facilitated the collapse of Milosevic's regime. It persuaded the Serbian leader that the NATO alliance had the political stamina to continue the air strikes and it convinced him that, "despite his best efforts at striking allied aircraft, his air defense system was inadequate and he would eventually lose."[19]

Despite the amount of ordnance expended, the air campaign was unable to stop Milosevic from continuing his atrocities against the Kosovar Albanians. This was partly due to the fact that "air strikes against dispersed or hidden targets were largely ineffective."[20] Without a ground invasion or a deception plan to draw out the Serbian force, they could maximize the use of their terrain and protect key elements of information, such as force location and high value assets like air defense systems, which are normally targeted to gain air superiority. This posed a significant problem for the Air Component Commander because without coalition ground forces, the Serbs through the use of cover, concealment, and deception had freedom of movement and held the initiative.[21] Fortunately, these lessons were observed and rectified in Afghanistan and Iraq.

While there were many lessons derived from this air operation, two are important to highlight. First, the air strategy of gradual escalation or incrementalism is not the most efficient

---

[18] Daniel Byman and Matthew Waxman. "Kosovo and the Great Air Power Debate". *International Security*, 24:4. MIT Press Journals. p. 31.

[19] Benjamin Lambeth (2001). *NATO's Air War for Kosovo; A Strategic and Operational Assessment*. Rand Project AIR FORCE: Santa Monica. p. 83.

[20] Ibid, p. 13

[21] Phone conversation with Lt Gen (retired) Short on 26 Jan 2007 stating it wasn't just enough to have the threat of a ground invasion but the Coalition needed an actual ground invasion to deny Milosevic his freedom of movement.

method for coercion, specifically against an enemy with a robust integrated air defense system like Serbia's. Using air power to coerce an enemy "focuses on affecting the enemy's will rather than negating his capabilities."[22] While this view supports Pape's argument that air power was less than efficient to coerce an enemy because breaking his will required total annihilation, it was never the Air Component Commander's intent to completely annihilate Serbia but rather gain a level of air superiority and strike the necessary axiological targets needed to coerce Milosevic to capitulate. The lesson is that axiological targeting along with a synchronized IO plan would have been a more efficient method of coercion given the constraint of no ground forces. As such, gradual escalation not only allowed Milosevic enough time to decipher our strategy and attempt to counter it, but also created challenges with identifying targets that would inflict enough pain to cause Milosevic to surrender.

While the Air Component Commander pushed for striking strategic targets throughout Kosovo and Serbia, the Combined Force Commander's (CFC) priority centered on Serbian military forces to stop the ethnic cleansing in Kosovo. Unfortunately without a ground invasion, Milosevic was able to maximize the use of terrain making it difficult for NATO aircraft to strike his fielded forces as well as his mobile air defense systems. Differences between the CFC and the Air Component Commander over targeting priorities or even broader, the enemy's center of gravity, further delayed NATO's ability to coerce Milosevic and increased its reliance on suppression of enemy air defense (electronic warfare) and intelligence, surveillance, and reconnaissance aircraft to protect allied aircraft and locate high value Serbian targets. Even still, these platforms were not optimized to find and fix fielded military forces. Finally, NATO never

[22] Horowitz, & Reiter (2001). When Does Aerial Bombing Work? Quantitative Empirical Tests, 1917-1999. The Journal of Conflict Resolution, Apr 2001. p. 149.

fully synchronized their IO campaign with the overall campaign objectives.[23] In this regard, Serbia held the upper hand in IO.

The second lesson learned focuses on the importance Serbia placed on IO in its strategy to counter US air dominance. Serbia's civil and military use of counter-information along with other integrated control enablers were aimed at delaying air superiority and breaking the fragile alliance. Other aspects of information warfare were also used. A report by Dr. Kevin O'Brien, a RAND Europe senior analyst, noted that Serbia conducted small scale, uncoordinated hacking, and computer network attacks targeting NATO's email and western government websites.[24] While these attacks against our command and control systems were relatively ineffective, it illustrated the full extent to which Serbia was committed to its asymmetric strategy. Finally, the use of decoys combined with the effects of weather and terrain on airborne sensors, essentially delayed allied air dominance. The US lesson is that more effective methods are necessary to conduct battle damage assessment as well as operational analysis during the targeting phase of planning. However, decoys and computer attacks were not the only IO tool that Milosevic chose to use.

The inadvertent air strike on the Chinese Embassy and the propaganda supplied by three captured US soldiers, became the influence operations center piece that Milosevic used to fuel his anti-coalition propaganda. In interviews conducted after the air campaign, the Serbs believed the air strike against the Chinese Embassy was deliberate and created a psychological effect on the Serbs that NATO was willing to strike anything to stop Milosevic.[25] While Milosevic worked hard to exploit NATO's errors, it was his own ethnic cleansing campaign that coalesced world

[23] P.W. Singer (2001). "Winning the War of Words: Information Operations in Afghanistan". Institute of Communication Studies, University of Leeds, United Kingdom.

[24] As cited by Dr. Kevin O'Brien, RAND Europe Senior Analyst. [electronic version: http://www.isodarco.it/courses/trento02/paper/trento02-brien_inf.pdf]

[25] Phone conversation with Lt Gen (retired) Short on 26 Jan 2007.

opinion against the Serbian leader. The amount of coverage provided by the media during Allied Force not only became the template for media operations for future wars but also broadcasted allied strengths and weaknesses in real-time to other countries.

Afghanistan and Operation Enduring Freedom (OEF)

Even though some analysts argue that "from the commencement of bombing on Oct. 7, 2001, through the Tora Bora campaign in December 2001, OEF was primarily an air war"[26], in fact, it was a combined arms effort. More accurately air power, combined with Special Operations Forces (SOF) and local irregular forces, collapsed the Taliban regime. What made air power so effective was the lethal combination of Special Forces (SF) and Air Force Combat Controllers working together to locate and target Taliban and Al-Qaeda forces. Additionally, the Taliban possessed few serviceable surface-to-air missile systems and anti-aircraft guns to effectively resist US air strikes.[27] That allowed the coalition to quickly establish air superiority and defeat the Taliban regime through a combination of precision air strikes and IO; specifically, the electronic warfare and influence components of IO. These operations ultimately achieved US military objectives.

President Bush defined the military objectives in his 7 October address to the country. He stated that the destruction of terrorist training camps, the capture of Al-Qaeda leaders, and the cessation of terrorist activities in Afghanistan were non-negotiable.[28] Based on those objectives, US Central Command (CENTCOM) began planning to "destroy the Al-Qaeda network inside Afghanistan along with the illegitimate Taliban regime which was harboring and protecting

---

[26] William Arkin. "Air head's: Misperceptions and rivalries obscure air power's potential". Armed Forces Journal. June 2006.

[27] Anthony Cordesman (2002). *The Lessons of Afghanistan; War Fighting, Intelligence, and Force Transformation*. Center for Strategic and International Studies. Washington DC. p. 15

[28] As cited from President Bush's 7 October 2001 Address to the country. [online version]. http://www.globalsecurity.org/military/library/news/2001/10/mil-011007-usia01.htm

terrorists."[29] The CENTCOM planners used the lessons of the Soviet Campaign in Afghanistan along with the Defense Secretary's desire for a swift response and developed an air and ground strategy to fit these objectives. That strategy led to many early successes.

The first task SOF executed was working by, with, and through tribal leaders to gain influence among the Northern Alliance to form these irregular fighters into a credible fighting force. By Air Force definition, these influence operations prepared and shaped the operational battle-space by convincing Alliance leaders to work with coalition forces and gathered critical intelligence needed to effectively tie the air campaign to a ground offensive. Once inserted, the SOF teams quickly organized an offensive using these irregular fighters against the Taliban.

Without conventional ground forces and minimal organic firepower, these teams were heavily reliant on air strikes for operational fires. The challenge for air power was to minimize the collateral damage to Afghan non-combatants through IO's integrated control enablers of ISR and precision navigation and timing. As a result, IO concerns shaped the war plan which "sought to rely to the fullest extent possible on precision-guided weapons."[30] According to Michael O'Hanlon, the "United States had flown about 25,000 sorties in the air campaign and dropped 18,000 bombs, including 10,000 precision munitions."[31] By the mid November 2001, there were roughly 17 SF teams in Afghanistan, Kabul was under US control, and the Taliban occupied less than one-third of the country. Despite achieving two out of the three stated goals, Al-Qaeda's leader Osama bin Laden was still at-large.

The tempo created by SOF targeting teams and precision air strikes forced the remaining elements of the Taliban to quickly disperse into the rugged terrain which created a new problem

---

[29] As cited from http://www.globalsecurity.org/military/ops/enduring-freedom.htm [online version].

[30] Benjamin Lambeth (2005). *Air power against terror: America's conduct of Operation Enduring Freedom*. Santa Monica: RAND Corporation. p. xvi

[31] Michael Hanlon (2002). "A Flawed Masterpiece". *Foreign Affairs Journal*, Vol 81(3), p. 48.

for coalition forces. Pockets of resistance began to emerge while the Taliban created safe havens in caves and mountains. Targeting the Taliban became difficult because they "dispersed in ways even the most advanced US ISR capabilities can not target and defeat."[32] Therefore influence operations, such as Army SF working through tribal leaders and other human intelligence assets, were critical in locating Taliban strongholds. In addition, It was also becoming clear that relying on surrogate or local forces for ground operations was becoming a risk due to corruption and conflicting loyalties. Both of these challenges, enemy dispersion and the use of surrogate forces, would create a long-term "struggle for Afghanistan [and] provided lessons to our enemies as well as for the US."[33]

The use of lethal along with non-lethal actions like psychological operations and counter-propaganda were effective in denying Taliban and Al-Qaeda forces sanctuary in Afghanistan and proved an important lesson for the US early in the campaign. Colonel Creighton[34] posits that psychological operations, civil-military operations, and ISR were "critical in preventing the re-emergence of terrorism on Afghan soil."[35] The combination of advanced ISR systems and human intelligence enabled the US to find and fix enemy sanctuaries and then conduct lethal operations eliminating them. Non-lethal actions such as civil-military and influence operations would follow to counter anti-coalition propaganda and assist with reconstruction efforts. When the non-lethal actions were not implemented, enemy sanctuaries re-emerged tying up more air and ground forces. While some critics warn that the US often over-emphasizes lethal, high tech methods of warfare to counter low-tech strategies, countries such as China "fully recognize the US approach

[32] Anthony Cordesman (2002). *The Lessons of Afghanistan; War Fighting, Intelligence, and Force Transformation*. Center for Strategic and International Studies. Washington DC. p. 26.

[33] Ibid. p. 28.

[34] Colonel James Creighton commands the 10th Mountain Division Artillery during Operation Enduring Freedom

[35] James Creighton (2004). "Effects Based Operations in Afghanistan: The CJTF-180 Method of Orchestrating Effects to Achieve Objectives". *Field Artillery Magazine*, January/February 2004. p.27.

to warfare and is aggressively modernizing their force"[36] to conduct a similar type of warfare that the US displayed in Afghanistan.

Iraq and Operation Iraqi Freedom (OIF)

Since the end of Desert Storm in 1991, air power has maintained a continued presence enforcing no-fly zones in northern and southern Iraq. The intelligence and experienced gained from 12 years of US air operations played a key role in General Franks' three-part operational strategy. Those air operations provided detailed information on Iraqi air defense operations and templated key Iraqi ground forces. Using that information, General Franks designed a strategy using ground maneuver, special operations, and precision fires simultaneously to defeat Iraqi forces and secure Baghdad.[37] Secretary of Defense Donald Rumsfeld supported the strategy in a testimony before the Senate stating that Franks "overwhelmed" the enemy using speed, jointness, precision, and intelligence. While the strategy maximized overwhelming power and speed, Dr. Stephen Biddle argues that precision, *situational awareness*, and poor Iraqi decision-making were the real sources behind the strategy's success.[38] US situational awareness was developed through what the Air Force calls predictive battlespace awareness. This is a process that develops an understanding of the operating environment through focused ISR, pattern analysis, and a continuous assessment. Dr. Krepinevich, the executive director for an independent research institute on defense planning, supports Biddle's argument claiming that "although achieving air

[36] Anthony Cordesman (2002). *The Lessons of Afghanistan; War Fighting, Intelligence, and Force Transformation*. Center for Strategic and International Studies. Washington DC. p. 30.

[37] Anthony Cordesman (2003). *The Iraq War; Strategy, Tactics, and Military Lessons*. Center for Strategic and International Studies: Washington DC. p. 3

[38] As cited from John Hopkins University lecture series entitled "U.S. Military Operations in Iraq: Planning, Combat, and Occupation". Dr. Stephen Biddle, Nov, 2005. http://www.sais-jhu.edu/merrillcenter/Panel1_Summary.pdf. Downloaded from website in January 2007.

superiority and gaining an information advantage were important priorities in the First Gulf War, US reliance on them was even greater in Operation Iraqi Freedom."[39]

Arguably, there were two main reasons why the US relied more on air and information superiority in OIF. First, the Iraq campaign relied heavily on air power to compensate for the paucity of ground forces; most senior military leaders believed more forces were necessary.[40] As a result, air power supplied the majority of the operational fires needed to enhance the lethality of this relatively small ground force. This, combined with the decision to launch the air and ground war nearly simultaneous, now required coalition air forces to quickly gain air superiority so more aircraft could support the ground offensive. US Central Command Air Forces estimated that 79% of all strike sorties during major ground combat operations were dedicated to close air support and interdiction missions.[41] Along with controlling the skies, US planners integrated operational security measures, deception operations, and other elements of information operations to conceal the size and location of the coalition force.

The second reason coalition forces emphasized air and information superiority stemmed from political considerations. The US declared that hostilities were aimed at the government of Iraq and not the Iraqi population requiring the coalition to "defeat the enemy regime without alienating its people."[42] To accomplish this, General Franks relied heavily on precision-guided munitions to reduce the probability of collateral damage. Most recent CENTCOM reports state 65% of all strikes were precision strikes compared to 35% in Operation Allied Force. However, this effort supported just one of four main objectives of OIF.

---

[39] Andrew Krepinevich (2003). "Operation Iraqi Freedom: A First-Blush Assessment". Center for Strategic and Budgetary Assessments: Washington DC. p. 14.

[40] Walter Boyne (2003). *Operation Iraqi Freedom: What Went Right, What Went Wrong and Why*. Tom Dougherty Associates: New York. p. 59. Boyne addresses the decision to strike with relatively small number of forces to prove Rumsfeld's concept of force transformation.

[41] Anthony Cordesman cited this data from Lt Gen Moseley

[42] As cited from http://www.csbaonline.org/4Publications/Archive/R.20030916.Operation_Iraqi_Fr/R.20030916.Operation_Iraqi_Fr.pdf and downloaded in January 2007.

From an air power perspective the military objectives as well as the air strategy were clear. Essentially, the US objectives in Iraq were to isolate and overthrow the Iraqi regime, destroy Iraqi weapons of mass destruction, protect our allies and supporters from Iraqi attacks, and destroy terrorist networks in Iraq.[43] Lieutenant General Michael Moseley, the air component commander, chose a strategy-to-task approach which efficiently linked air power tasks to campaign objectives. This methodology quickly adapted to changes in the ground situation by ensuring each component's high priority targets were serviced. However, Anthony Cordesman estimated that 35% of the requests for attack sorties were rejected "in an effort to limit the destructiveness of the air campaign."[44] Overall, the air strategy was not designed to bomb a country but rather, it sought to paralyze a regime and effect the Iraqi military as a system.

The effect from 12 years of continued air operations leading up to the ground offensive provided the coalition with a significant advantage over Sadam's military. By most accounts, the US and British air forces not only "defeated the Iraqi Air Force… [but also] heavily suppressed the Iraqi land-based air defense systems before the war began."[45] This gave the air component an almost infinite force ratio advantage in terms of military effectiveness and enabled coalition air forces to focus on close air support and air interdiction missions early on in the war. Even still, "coalition planners underestimated the psychological effects precision firepower had on Iraqi combat units."[46] Through interviews with senior Iraqi Commanders, the US learned exactly how lethal air power was from the Iraqi perspective.

---

[43] USCENTAF, Assessment and Analysis Branch. 30 April 2003. "Operation Iraqi Freedom – By the Numbers". p. 4

[44] Anthony Cordesman (2003). *The Iraq War; Strategy, Tactics, and Military Lessons*. Center for Strategic and International Studies: Washington DC. p. 27.

[45] Anthony Cordesman (2003). *The Iraq War; Strategy, Tactics, and Military Lessons*. Center for Strategic and International Studies: Washington DC. p. 28.

[46] US Joint Forces Command, "Iraqi Perspectives Project". p. 125

The effects of both precision air strikes and psychological operations made the Iraqi's feel "like they were constantly in a sniper's sight."[47] The commander of the Republican Guard I Corps stated "the level of precision in those [air] attacks put real fear into the soldiers of the rest of the division."[48] A sense of helplessness quickly swept through the Iraqi military when US and allied aircraft dropped leaflets on their exact location with messages targeted directly to that unit and Iraqi air defenses could not stop these incidents. The Al-Nida Commander best summarized the effect of US air power on the Iraqi military when he stated:

> "The air attacks were the most effective message. The soldiers who did see the leaflets and then saw the air attacks knew the leaflets were true. Overall, they had a terrible effect on us. I started the war with 13,000 soldiers…and by the time we had orders to pull back to Baghdad, I had less than 2,000 [and] still had no engagements with American forces."[49]

According to the Iraqi ground commanders, air power was decisive in defeating their conventional forces. However, given all the advantages that air power held, there were still challenges associated with targeting a dispersed enemy.

Even though air interdiction missions, which were enabled by precision weapons and ISR, successfully paved the way for the ground offensive, air power alone could not effectively defeat Saddam's irregular forces. Without ground forces confirming target data, airborne ISR by itself could not positively distinguish between conventional and unconventional forces. While air power weakened Iraq's conventional military ahead of coalition ground forces, unconventional forces like the Fedayeen and the Ba'ath militia conducted random attacks on the coalition's rear supply lines. Had these attacks by irregular forces been better coordinated or properly focused on logistic chokepoints, these forces could have drastically slowed the coalition's advance. Even though General Franks declared that "precision and information were the clear winners in OIF",

[47] US Joint Forces Command, "Iraqi Perspectives Project". p. 125
[48] Ibid. p. 125
[49] Ibid. p. 126.

more work must be done to integrate both of these areas with non-lethal elements to effectively counter asymmetric threats especially in the context of counter insurgency operations.

Having examined three air campaigns, it is clear that IO has played an increasingly important role in military strategy. As the importance of IO continues in future conflicts, more emphasis will be placed on not only supporting the technical components of IO through advances in technology, but also in developing a holistic understanding our adversary which enhances the non-lethal aspects of IO. The following chapters examine how China and Russia define and use the technical and non-technical forms of IO to counter future US air dominance.

CHAPTER THREE

CHINA

China's Strategic Context

Dr. Avery Goldstein writes, "China is the post-Cold War world's emerging great power that poses the most difficult questions for the future of international security."[50] The 2006 Quadrennial Defense Review addresses some of those security concerns stating, "China has the greatest potential to compete militarily with the US and field disruptive military technologies that could over time offset traditional US military advantages."[51] Specifically, the Chinese are investing in information technology to not only modernize their military but also to develop their technical component of IO. From 1990 to 2000, the Chinese information technology sector grew nine-fold "registering the fastest growth rate among the country's industrial sectors."[52] As China's military power grows, the US places more importance on understanding their capabilities and intent. This chapter examines how IO fits in China's strategic context, explains the role of IO in Chinese military, and analyzes how IO affects their military doctrine and organization.

Making sense of China's strategic context is no simple task, yet crucial for understanding how IO fits into China's military modernization. While most analysts claim, "the focus of United States-Chinese security concerns has long been the Taiwan Straits"[53] they are quick to recognize that conditions are changing. A more troubling reality for the US is China's growing industrial base and energy production. If China can translate this growth into their defense industry, China

[50] Avery Goldstein. "Great Expectations: Interpreting China's Arrival". *International Security*. Vol 22, No. 3. p. 36.

[51] Department of Defense (2006). "Military Power of the People's Republic of China". p. I. [electronic version], downloaded from http://www.defenselink.mil/pubs/pdfs/China%20Report%202006.pdf in January 2007.

[52] Adam Segal (2002). "Digital Dragon. High Technology Enterprises in China". Council on Foreign Relations: Cornell. p. 3.

[53] Stephen J Blank (2006). "China's Military Power: Shadows Over Central Asia". The Lexington Institute: Arlington, p. 2.

will have the means to sustain military operations against a potential adversary. Their military reform looks to capitalize on this sustainment by examining strategies for conducting long term, protracted military operations in which information technology plays a key role. This military reformation is currently underway.

Jiang Zemin, former President of the People's Republic of China, noted before the start of the Iraq War that the People's Liberation Army (PLA) must pursue an "informationized" force alongside a "mechanized" force.[54] What exactly does that mean? Mechanization as a product of the industrial revolution relies on China's industrial capacity to mass-produce military equipment and supports maneuver warfare by providing greater mobility and firepower. Arguably, the PLA were never fully mechanized because they lacked both the industrial capacity and the economic resources to do so. "Informationization"[55] is the use of new information technologies to increase the lethality of weapons and streamline command and control. Accepting that premise now leads to the belief that better information systems enables smaller, more agile forces capable of results that are greater than the sum of their parts. However, to understand the full impact of informationized forces and the Chinese threat, its power must be interpreted.

Tracking defense spending is one way of interpreting Chinese military power. US budget analysts reported that China's defense budget increased 14.7% in 2006 which "continues a trend of double-digit growth since 1990."[56] Even though the PLA is reducing its military by 200,000 troops[57], they continue to procure new weapon systems, upgrade their older equipment, and

---

[54] The National Institute for Defense Studies (2004). "China-In Search of New Thinking", *East Asian Review 2004*. The Japan Times, Ltd: Tokyo. [electronic version].

[55] The Chinese continue pursuing a mechanized and an "information-ized" military force. This "information-ized" force focuses on networking their command and control systems and their weapons.

[56] Department of Defense (2006). "Military Power of the People's Republic of China". p. 19-20. [electronic version: http://www.defenselink.mil/pubs/pdfs/China%20Report%202006.pdf] downloaded in January 2007.

[57] Information Office of the State Council of the People's Republic of China, "China's National Defense in 2006", Beijing *Xinhua Domestic Service*, 29 Dec 2006. downloaded from www.opensource.gov CPP20061229704001 in January 2007.

invest in training their soldiers. Whether or not China can keep up the pace of its modernization remains an important question for defense officials but defense spending by itself does not address the intent behind its military build up.

By studying the past, the Chinese have learned to attach greater importance to absorbing the actual war experiences of militarily strong countries for lessons that can counter US air power and eventually incorporate them into their doctrine. [58] Changes in doctrine and organization also provide insight on *why* the Chinese military is reforming. Dr. Dennis Drew explains this premise by noting that changing circumstances like significant world events or new technologies influence doctrine and "must be continually evaluated because they can modify beliefs about the important lessons of experience."[59] For example, the Chinese paid close attention to the post-Gulf War debates over the efficacy of air power alone to achieve national goals. The details of this debate convinced the Chinese that air power, along with new information technology posed a significant threat and doctrinally "switched [their] philosophy [of their air force] from defense of national territory to both offense and defense."[60] However, the greatest influence on Chinese strategy and doctrine comes from the advances in information technology and its impact on IO.

The Chinese observed a growing US dependence on precision munitions and IO.[61] Major General Pufeng Wang, Director of the Strategy Department, Academy of Military Science stated "we recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness...this trend will be highly critical to

---

[58] Tian Xin, "Effects of US War in Afghanistan on China's Military Thinkers", *Wen Wei Po*, 4 Feb 2002. downloaded from FBIS (www.opensource.gov) CPP20020204000032 in January 2007.

[59] Dennis Drew (LtCol, Ret) and Don Snow (1988). *Making Strategy: An Introduction to National Security Processes and Problems*, pp. 163–174. Montgomery: Air University Press.

[60] The Hudson Institute (2005). "China's New Great Leap Forward: High-Tech and Military Power in the Next Half Century", Hudson Institute: Cicero. p. 35.

[61] Wang Hucheng, "The US Military's 'Soft Ribs' and Strategic Weaknesses", Liaowang: Issue 27, 5 Jul 2000.

achieving victory in future wars."[62] As such, Chinese information warfare (IW) theory provides some insights on not only the modernization efforts of the PLA but also provide an understanding of how the Chinese define future war.

Early views of Chinese IW closely resembled US definitions. In 1999, Major General Dai Qingmin, commander of the PLA's Information Warfare Center in Wuhan, defined IW as having six forms consisting of operational security, military deception, electronic warfare, psychological warfare, computer network warfare, and physical destruction. As information technologies matured, he began challenging the traditional Chinese military strategy of active defense by "advocating pre-emptive attacks to gain the initiative and seize information superiority."[63] Essentially, China's growth in information technology drove IW's three technical forms which are electronic warfare, computer network warfare, and physical destruction (precision munitions). Through the use of stratagems, China combines those forms with its three non-technical forms which are operational security, military deception, and psychological warfare as a complete IO strategy. In 2002, Dai refines his IW philosophy emphasizing the importance of electronic warfare and computer network attack. This integration clearly focuses on the kinetic aspects of IW—consistent with the lessons the Chinese observed up through the Kosovo War. However, other views of Chinese IW takes their origins from Marx.

Chinese IW, as a subset of People's War under high-technology conditions,[64] has an asymmetric component in which "two sides using information control and intelligence fight for

---

[62] Major General Wang Pufeng (1995). "The Challenges of Information Warfare". [electronic version]. http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm downloaded in January 2007.

[63] Timothy Thomas (2001). "China's Electronic Strategies". *Military Review*. May/June 2001 [electronic version]. http://leav-www.army.mil/fmso/documents/china_electric/china_electric.htm downloaded in October 2006.

[64] Hsien-Tai Chun-Shih, "China's Major General Wang Pufeng Discusses Definition, Significance of Information Warfare", PRC Monthly Journal covering international and Chinese military affairs. 11 April 2000. p. 19-21. Accessed from https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_246_203_0_43 in January 2007.

the initiative in war."[65] Dai emphasizes that asymmetry exists in using technical versus the non-technical means and vice-versa to establish information control which will become the dominant focus of future wars and the main requirement for gaining the initiative in information warfare.[66] This concept of initiative along with sustaining the offensive plays an important part in the theory of People's War. People's War is a Marxist term used to describe a strategy of protracted war employed by the people for liberation against an aggressor. The Chinese believe that IW, like people's war, contains many asymmetric qualities.

In People's War, Mao redefined power giving partisans an asymmetric edge. Instead of quantifying power in terms of material, he believed the quantity of people and the will of the people were key sources of power. Mao claims that "weapons are an important factor in war, but not the decisive factor; it is people, not things, that are decisive."[67] Beijing has defined a "new concept of people's war [that] includes IT warriors from not only the 2.5 million strong army, but also from the general citizenry of some 1.3 billion people."[68] Because of the relatively large number of people (information nodes) and advances in information technology, the Chinese believe IW has redefined power and now provides them a key asymmetric advantage. The lessons from the air campaigns over the past ten years reinforce this belief.

Chinese Lessons from Kosovo

The air campaign in Kosovo offered some insights to the Chinese for developing strategies to counter US air power. According to Dr. Toshi Yoshihara, a senior research fellow at

[65] [No author provided]. "Taiwan Report on PRC Development on Laws of Armed Conflict", *Taiwan Defense Affairs*, 1 Sep 2004. [electronic version cited from www.opensource.gov]

[66] Timothy L. Thomas (2005). *Cyber Silhouettes: Shadows Over Information Operations.* Foreign Military Studies Office: Leavenworth. p. 83.

[67] Mao Tse-tung, "On Protracted War," *Selected Military Writings of Mao Tse-tung* (Peking: Foreign Languages Press, 1968), pp. 217

[68] Victor N Corpus. "Part 1: Striking the US Where It Hurts", *Asia Times Online.* 18 Oct 2006. [online version] accessed in January 2007.

the Institute for Foreign Policy Analysis, "Chinese observers have scrutinized the Kosovo conflict with great interest to distill lessons learned on potential defensive strategies"[69] and concluded that IW is one possible method of countering US air power. The Chinese noted the information domain primarily supported physical destruction and electronic attack. Dr. Yoshihara's research stated that "Chinese strategists unanimously concur that enhancing defense against physical [IW] attacks are critical requirements for Chinese IW [and also agree] that offensive and defensive elements of IW require a robust and effective command and control system."[70]

According to Maj. Gen. Dai Qingmin, when a strong defense and an effective command and control system are in place, one can render an adversary "blind and deaf". That is, when deception, operational security, and electronic warfare are integrated into defenses, one can "lure" his adversary into situations that are undesirable. Lieutenant General Yazhou provides an example of how IO can render an adversary "blind and deaf":

> "In the 1999 Kosovo War, the commander of the air force of the Federal Republic of Yugoslavia piloted a MiG fighter, trying to fight a battle with NATO fighters. But, the Yugoslavian radar was disturbed and the correspondence to and from the MiG fighter was interrupted. The commander could not see where his enemy was. So the MiG fighter was shot and crushed by a Netherlander fighter soon after it took off. Another five MiG fighters were also downed 5 minutes after taking off. Even most anti-air missiles would have less than 5 minutes of survival time."[71]

This reinforces the lesson that synchronizing IO with a "robust air defense is viewed as a critical component for supporting offensive forces."[72] Does this lead to the idea that the greater our information technology, the stronger our offensive forces become? Not exactly.

---

[69] Toshi Yoshihara (2001). "Chinese Information Warfare: A Phantom Menace or Emerging Threat?", Strategic Studies Institute: Carlisle. p. 15.

[70] Toshi Yoshihara (2001). "Chinese Information Warfare: A Phantom Menace or Emerging Threat?", Strategic Studies Institute: Carlisle. p. 15.

[71] Liu Yazhou, Lieutenant General PLAAF, "China-America: The Great Game", *Eurasian Review of Geopolitics*, Jan 2005. p. 20.

[72] Stephen J. Flanagan and Michael E. Marti (2003). *The People's Liberation Army and China in Transition*. National Defense University Press: Washington DC. p. 165.

The air campaign also demonstrated how information technology can enhance the lethality of weapon systems as well as create vulnerabilities in such a high-tech force. Dai noted that "as the informationization of an enemy advances, its reliance on information rises and its vulnerability increases, so that attacks on an enemy's [combat information system] are [more] effective."[73] Now simple, low-tech solutions applied against combat information systems are countering advanced, information-based weapon systems. One Chinese military analyst cited an example that supports how low-tech counters the high-tech when the Serbs used operational security and deception to confuse NATO collection, targeting, and air strikes.

> "During the war in Kosovo, the Yugoslav Federation countered infrared guided weapons by using sheet iron heated red-hot, it countered laser-guided weapons using smoke from burning old tires, and it countered stealth airplanes using old-style meter-wave radar."[74]

These seemingly low-tech measures played an important role in frustrating US air power and bought time for Milosevic to continue his anti-coalition campaign. China also understands that even though Serbia succeeded in shooting down two US aircraft, that alone had little impact on the outcome of the war. It did, however, prove that weaknesses in information technology and equipment can be exploited.

The Chinese also agree that while precision guided munitions "hit 69 percent of targets in Desert Storm and 85 percent in Desert Fox, they hit only 20 percent in Kosovo—the failure to hit those targets was due not to inaccuracy, but to an ingenious deception campaign."[75] While this strategy worked well for some mobile targets, Precision Guided Munitions were very effective against fixed targets. For that reason, Major General Zheng Shenxia, president of the Chinese Air

---

[73] The National Institute for Defense Studies (2004). "China-In Search of New Thinking", *East Asian Review 2004*. The Japan Times, Ltd: Tokyo. p. 111.

[74] Dai Qingmin, Maj. Gen. PLAAF. "On Seizing Information Superiority", Beijing *Zhongguo Jungshi Kexue*, 20 April 2003. downloaded from www.opensource.gov, CPP20030728000209 in January 2007.

[75] The Hudson Institute (2005). "China's New Great Leap Forward: High-Tech and Military Power in the Next Half Century", Hudson Institute: Cicero. p. 48.

Force Command College, believes that "future IW will rely more and more on air superiority"[76] to essentially fix in place high-value targets. Afghanistan is one clear example of how information, land, and air warfare combined to render an adversary blind and deaf and defeat a regime.

Chinese Lessons from Afghanistan

Beijing viewed Afghanistan as a watershed for both information and traditional warfare.[77]

The information war, enabled by advances in information technology, improved precision strikes and set new limits on networked command and control (computer network warfare). This is a critical development needed for China's goal of "informationization" and supports what Colonel Gaihe calls a "Strategy of Comprehensive Integration". The PLA contend that comprehensive integration will "use information technology to improve weapon systems and combat forces, enhancing their links and coordination in order to heighten their overall combat effectiveness."[78] Essentially, comprehensive integration is similar to a "system of systems" approach with the goal of making the PLA more efficient and effective through information technology. The early success in Afghanistan validated China's concept of comprehensive integration.

Chinese analysts also attribute coalition success in Afghanistan to small, elite ground forces that effectively executed the information war and leveraged air power to deny the Taliban their command and control and freedom of movement.[79] These elite units or special operations forces, organized the resistance in the north, created a southern alliance, and assisted in

[76] Jacqueline A. Newmeyer, "China's Air Power Puzzle", *Policy Review*, Jun/Jul 2003. p. 72

[77] Tian Xin, "Effects of US War in Afghanistan on China's Military Thinkers", *Wen Wei Po*, 4 Feb 2002. downloaded from FBIS (www.opensource.gov) CPP20020204000032 in January 2007.

[78] Ibid.

[79] The Hudson Institute (2005). "China's New Great Leap Forward: High-Tech and Military Power in the Next Half Century", Hudson Institute: Cicero. p. 29.

neutralizing the Taliban's command and communications systems.[80] They achieved this success using psychological warfare, irregular warfare[81] and physical destruction. One PRC-owned newspaper ran an article that focused on the impact these elite units made using IO:

> "The first thing the US military threw into the battlefield in Afghanistan was not bombs but information war equipment used to intercept intelligence information. The armed forces the United States first committed on the ground in Afghanistan weren't mountain divisions but were Special Forces and psychological operations troops used to obtain intelligence."

The key to success for these forces was establishing credibility by obtaining relevant intelligence about the enemy's location and size as well as fighting alongside the indigenous forces. Often times, their weapons were a radio and a laser pointer for conducting targeting operations for precision air strikes or the Chinese IO form of physical destruction.

According to General Yazhou, the air strikes not only "paralyzed their nervous system" by destroying critical targets but also denied the Taliban forces freedom of movement. While Tora Bora and Operation Anaconda show that the US should do more to limit the mobility of enemy forces, China's leaders still believe that "precision bombing accelerated the progress of the war, and timely intelligence accelerated the collapse of the Taliban defense system."[82] Maj. Gen. Dai summarized these lessons of integrating precision air strikes (physical destruction), IW and elite forces noting:

> "…information supremacy is a prerequisite for seizing and maintaining air and sea supremacy. Because the air and sea battle spaces rely very heavily on

---

[80] Tian Xin, "Effects of US War in Afghanistan on China's Military Thinkers", *Wen Wei Po*, 4 Feb 2002. downloaded from FBIS (www.opensource.gov) CPP20020204000032 in January 2007.

[81] Irregular Warfare, as defined by the Multi-Service Concept for Irregular Warfare, 2 August 2006 is a form of warfare that has as its objective the credibility and/or the legitimacy of the relevant political authority with the goal of undermining or supporting that authority. Irregular Warfare favors indirect approaches, though it may employ the full range of military and other capabilities to seek asymmetric advantages to erode an adversary's power, or will.

[82] Tian Xin, "Effects of US War in Afghanistan on China's Military Thinkers", *Wen Wei Po*, 4 Feb 2002. downloaded from FBIS (www.opensource.gov) CPP20020204000032 in January 2007.

> information systems, to seize air and sea superiority it is first essential to paralyze the enemy's information systems, while protecting one's own."[83]

General Yazhou agrees with Dai claiming that one major flaw with the US Air Force is that their reliance on information technology has scarred their warring tactics making them more and more rigid as well as allowing new technologies to drive their tactics.[84] Liu is not implying that China should abandon its pursuit of information technology however, China must not allow technology to dominate their warfighting principles.

Chinese Lessons from Iraq

Professor Zhang Zhaozhong of the Chinese National Defense University claims the greatest lesson learned from Iraqi Freedom is the importance of IW and its integration with other forms of war. He stated, "information warfare should not be conducted solely in the sphere of computer networks, but should proceed in coordination with traditional mechanized modes of warfare."[85] Operation Iraqi Freedom did just that. The air war in Iraq incorporated many aspects of IW, such as electronic attack and psychological operations, and synchronized those aspects with the land component's objectives. Most Chinese defense analysts, including General Yazhou whose comments are below, agree that US successes early on in Iraqi Freedom came from the use of air power stating:

> "I believe that air power was the decisive force for the Iraqi War, though the US sent massive ground forces as well. The US had global interests and hence broad war areas. It had to adopt a global strategy [and] made it essential for its armed forces to fight long-distance wars to be able to be deployed promptly, strike

[83] Dai Qingmin, Maj. Gen. PLAAF. "On Seizing Information Superiority", Beijing *Zhongguo Jungshi Kexue*, 20 April 2003. downloaded from FBIS CPP20030728000209 in January 2007.

[84] Liu Yazhou, Lieutenant General PLAAF, "China-America: The Great Game", *Eurasian Review of Geopolitics*, Jan 2005. p. 22.

[85] The Hudson Institute (2005). "China's New Great Leap Forward: High-Tech and Military Power in the Next Half Century", Hudson Institute: Cicero. p. 67.

> precisely and maintain absolute mastery of the sky. Among all parts of the US armed forces, only its air power could match those requirements."[86]

Unlike General Yazhou, the Iraqi Perspectives Project claim that speed, precision, and the combined use of air and information warfare was the decisive force that broke the will of the Iraqi military. However, this level of speed and precision through air and information was achieved largely through twelve years of previous "no-fly" operations in northern and southern Iraq and also because the Iraqi Air Force was essentially defeated before the war even started.

Iraqi Freedom reinforced China's commitment to continue the direction of its "military change with Chinese characteristics" stressing mechanization alongside the informationization of the armed forces. Beijing also claims that the future modernization of the PLA will most likely consist of a combination of both symmetric and asymmetric capabilities.[87] This new strategy is evident in their doctrine and organization.

Changes in Chinese Military Doctrine

Understanding how Chinese doctrine has changed due to IO requires a basic knowledge about how the Chinese view doctrine. A study of PLA doctrine by Georges Tan Eng Bok suggests that Chinese doctrine is better understood as Chinese military thought. Military thought, by their definition, reflects different "political and philosophical values…about war [and] shows the nature of war, its law of development, and fundamental principles for the building and employment of armed forces."[88] Their writings on military thought are structured similar to Russian doctrine in that the Chinese have socio-political and military-technical aspects of war. It

[86] Liu Yazhou, Lieutenant General PLAAF, "China-America: The Great Game", *Eurasian Review of Geopolitics*, Jan 2005. p. 11.

[87] The National Institute for Defense Studies (2004). "China-In Search of New Thinking", *East Asian Review 2004*. The Japan Times, Ltd: Tokyo. [electronic version].

[88] Ka Po Ng (2005). *Interpreting China's Military Power: Doctrine Makes Readiness*. Frank Cass of Taylor & Francis: New York. p. 19.

differs from Soviet and US doctrine in that the Chinese take a philosophical approach to examine these two aspects of war. In general, the socio-political area has remained relatively constant while the military-technical aspect continues to change. It is in the military-technical realm that IW has modified the PLA's context of war. Even still, the structure of Chinese military thought is dynamic enough to accommodate these changes since the writings on military thought serve as "the collective wisdom of Chinese Communist leaders."[89]

The collective wisdom captured in doctrine traces the evolution of Chinese military thought through four distinct phases: People's War; People's War under modern conditions; Local War; and Local War under high-tech conditions. Each phase represents the Chinese philosophy of maintaining military relevance to ensure their national security. As such, their doctrine "conveys the dynamic relevance of a changing international security environment."[90] For China, advances in information technology along with its global reach, make IW and air power dominant tools for ensuring China's national security in a dynamic environment. What China has struggled with the most is keeping pace with the speed of these changes. In a report to Congress on the military power of China, one analyst states:

> "China has devoted considerable effort to develop military strategy and doctrine to meet evolving conditions in the world. Yet analysis of Chinese writers' extensive study of coalition operations in Iraq and Afghanistan suggests China continues to be surprised at the rapid pace of change in modern warfare."[91]

Defining modern warfare may be part of the reason that China struggles to keep pace with its changes. At one end of the spectrum of conflict is local war which China describes as structured, organized, and regional. At the other extreme lies people's war characterized by mass

---

[89] Ka Po Ng (2005). *Interpreting China's Military Power: Doctrine Makes Readiness*. Frank Cass of Taylor & Francis: New York. p. 19.

[90] Ibid. p. 21.

[91] Department of Defense annual report to Congress: "Military Power of the People's Republic of China". 2006. p. 16.

mobilization for national survival. Both philosophies of war exist regardless of high-tech or low-tech conditions. Even though China's doctrine now states the need to gain information superiority, the current debate is determining if "informationization" simply defines a condition of war or generates a new philosophy of war.[92] The global reach and transparency of IW lead some Chinese analysts to believe that IW has essentially defined a new type of "non-contact" war. These analysts claim that non-contact war requires "innovative military theories [to] disengage from the traditional contact war model and break new ground [in] joint operations, integrated air and space warfare, and information network warfare."[93]

As stated earlier, both the Gulf War and the Kosovo War displayed new conditions and subsequently, changed some aspects of Chinese military thought. Specifically, "the Chinese air force switched its philosophy from defense of national territory to both offense and defense."[94] Their doctrine now reflects this change and "stresses high-tech, multi-role platforms capable of offensive and defensive operations."[95] One example of this doctrinal change is reflected in an organization modification of the China's Air Force to acquire the advanced, multi-role Su-30MKK fighter aircraft and are also producing their own 4th generation fighter, the F-10. However, this methodology of lessons formulating doctrine which produce equipment is not always the case.

The lessons from Afghanistan showed the Chinese that information technology could improve precision strikes (physical destruction) and network or flatten command and control (computer network wafare). The speed at which the US collapsed the Taliban command and

---

[92] Wang Pufeng, Major General. "China's Major General Wang Pufeng Discusses Definition, Significance of Information Warfare". *Hsien-Tai Chun-Shih*. 11 April 2000. downloaded from www.opensource.gov, 12/14/2006 CPP20000503000133

[93] The Hudson Institute (2005). "China's New Great Leap Forward: High-Tech and Military Power in the Next Half Century", Hudson Institute: Cicero. p. 46.

[94] Ibid. p. 35.

[95] Stephen J. Flanagan and Michael E. Marti (2003). *The People's Liberation Army and China in Transition*. National Defense University Press: Washington DC. p. 139.

control network and defeated their forces reinforces the idea that information superiority is essential for gaining the initiative in war. China's concept of local war "calls for a quick response to seize the initiative"[96] and emphasizes efficiency. In late 2003, the *PLA journal* published a study which calls for information technology to support joint operations in three areas: network and electronic warfare; active offense; and partial information dominance.[97] Network warfare not only refers to command and control but also computer attacks while active offense incorporates physical destruction and special forces. In this case, the lessons showed the Chinese that existing capabilities could support their philosophy of war with just a small change to their doctrine (the three areas of IW). The Iraq War in 2003 highlighted other methods of ensuring Chinese national security using information warfare.

China's strategic thought now includes rapid reaction forces and stresses joint operations because of the successful US invasion of Iraq.[98] These principles are consistent with China's lessons from the Iraq war in that IW must be integrated with other traditional mechanized forms of warfare. These rapid reaction forces are highly mobile, information-based units who operate with other PLA forces. Authors Wang Meiquan and Liao Jianlin debate this joint, reaction force claiming the PLA's top priority task "is not building up a joint tactical corps but making efforts to organize integrated training under information warfare conditions."[99] Operating under IW conditions allows the Chinese to quickly and accurately respond to modern war threats such as precision air strikes (physical destruction).

---

[96] Ka Po Ng (2005). *Interpreting China's Military Power: Doctrine Makes Readiness*. Frank Cass of Taylor & Francis: New York. p. 83.

[97] Ke Zhansan, "Studies in Guiding Ideology of Information Operations in Joint Campaign", Beijing *Zhongguo Junshi Kexue*, 20 Apr 2003. downloaded from www.opensource.gov, CPP20030728000210 in January 2007.

[98] A.F. Klimenko, "The Evolution of China's Military Policy and Military Doctrine", *Military Thought*, April-June 2005. [electronic version]. http://www.findarticles.com/p/articles/mi_m0JAP/is_2_14/ai_n15623000/print accessed in October 2006.

[99] Wang Meiquan and Liao Jianlin. "PLA Prudently Discuss Joint tactical Corps", *Jiefangjun Bao* (Internet Version - WWW). 10 May 2005. downloaded from www.opensource.gov in January 2007.

China's White Paper on National Defense describes their post-Iraq military strategy which contains terms such as strategic borders (sphere of influence) and active defense to counter any US preemptive action against China's national interests.[100] While these terms may not be new to the Iraq War, concepts such as joint operations, IW, and rapid reaction forces clearly fit into local war doctrine and enable China to maintain their sphere of influence or "strategic borders".[101] If China's national interests are promoting national unity, ensuring economic growth, and expanding their energy resources, then the lessons from Iraq provide a military strategy for these new capabilities under local war with high-tech conditions. In this case, the lessons of Iraq changed IW doctrine by integrating IW with traditional mechanized modes of warfare to produce new capabilities in the PLA (rapid reaction forces in joint operations).

Changes in China's Military Organizations

As the PLA moves toward informationization alongside mechanization, changes in the organizational structure and manpower continue. There are two main organizational areas the Chinese changed based on the lessons learned over the past ten years of US air operations and the advances in information technology. China's leaders have comprehensively reformed their Air Force and IW organizations. To understand the impact of these changes, it is necessary to have a baseline understanding of their structure.

The basic military structure resembles the former Soviet model that establishes military regions throughout the country. Prior to 1999, the Central Military Commission (CMC) led three general departments; the General Staff Department, the General Political Department, and the

[100] Information Office of the State Council of the People's Republic of China, "China's National Defense in 2006", Beijing *Xinhua Domestic Service*, 29 Dec 2006. downloaded from www.opensource.gov CPP20061229704001 in January 2007.

[101] A.F. Klimenko, "The Evolution of China's Military Policy and Military Doctrine", *Military Thought*, April-June 2005. [electronic version]. http://www.findarticles.com/p/articles/mi_m0JAP/is_2_14/ai_n15623000/print accessed in October 2006.

General Logistics Department. In 1999, the General Armament Department became the fourth department added as a "key measure for paving the way for a 21st century Army while keeping in mind…new military challenges."[102] Each region maintains elements of the Chinese armed forces composed of the "PLA, the People's Armed Police, and the militia."[103]

The PLA is composed of an Army, Navy, Air Force, and the Second Artillery. Over the past several years, advances information technology and observations of other conflicts changed organizational structures, roles, and force levels of the PLA. One observation the Chinese made during the Iraq War demonstrated the US ability to rapidly deploy combat forces and provide operational fires with global strike operations. This rapid response capability caused the PLA to examine its own organization and fighting capacity. However, real change required a top-down review of the PLA from a higher authority.

According to a 2003 *Open Times* article, the CMC assessed the lessons gained from the Iraq war and proposed a four-part military reformation plan. The reformation plan, known as "the Implementation of Strategic Project of Military Talents" focused on "building an informationized army and wining an information war."[104] The plan called for the personnel end-strength of no more than 2 million troops that means cutting an additional 500,000 troops. Maj. Gen. Ku Guisheng, vice dean of the PLA National Defense University, later confirmed the report stating, "as reform progresses, the organizational structure of the PLA would be optimized, and its overall size would be reduced."[105] However, the 2006 White Paper on National Defense reports that the PLA end-strength as 2.3 million troops which raises questions about the progress of the reformation plan.

---

[102] Pai Chuan, "Command System of the Chinese Army", Hong Kong, *Ching Pao* No 257, 01 Dec 1998. [online]. Downloaded from www.opensource.gov, FTS19981212000281 in January 2007.

[103] Ibid.

[104] The National Institute for Defense Studies (2004). "China-In Search of New Thinking", *East Asian Review 2004*. The Japan Times, Ltd: Toyko. p. 114-115.

[105] The National Institute for Defense Studies (2004). "China-In Search of New Thinking", *East Asian Review 2004*. The Japan Times, Ltd: Toyko. p.113.

The CMC led the PLA's reorganization effort by "reducing the number of military area commands from eleven to seven, and reorganized its infantry-heavy army into combined group armies composed of armored and mechanized or motorized infantry units."[106] These former provincial military districts will now adopt the new responsibility of territorial defense and will include an organic logistics and supply system to optimize their defensive posture. The savings generated from this reform is currently reinvested in upgrading "equipment and enhancing the technology level of the military to meet the requirements of the wars in the new period."[107] The next part of their information-based, reformation plan optimized the Air Force.

The People's Liberation Army Air Force (PLAAF) devised an aggressive modernization plan based on the lessons of previous air campaigns to build an information-based air force. The first step was retiring their older, second-generation aircraft and acquire more advanced, fourth-generation multi-role fighters. The end result of this upgrade "downsizes [the PLAAF] combat aviation fleet by 20 percent to 25 percent [however] their air strike capability should grow 50 to 70 percent as more advanced aircraft are accepted for service."[108] According to China's White Paper on National Defense for 2006, the PLAAF's goal is an informationized air force equipped with advanced armament, a precision strike capability, and enhanced command and control.[109] However, countering US air dominance requires more than just new, "informationized" aircraft.

China's integrated, information-based air defense network and growing culture of decentralized execution in the PLAAF complements these new aircraft and requires significant changes in the PLAAF's organization. Colonel Dai Xu touched on this same issue in an article

---

[106] The National Institute for Defense Studies (2004). "China-In Search of New Thinking", *East Asian Review 2004*. The Japan Times, Ltd: Toyko. p.114.

[107] Ibid. p. 114.

[108] A.F. Klimenko, "The Evolution of China's Military Policy and Military Doctrine", *Military Thought*, April-June 2005. [electronic version]. http://www.findarticles.com/p/articles/mi_m0JAP/is_2_14/ai_n15623000/print

[109] Information Office of the State Council of the People's Republic of China, "China's National Defense in 2006", Beijing *Xinhua Domestic Service*, 29 Dec 2006. downloaded from www.opensource.gov CPP20061229704001 in January 2007.

that compared these efforts to the US F-22 and stealth technology. Even though he over-states the capability of the F-22, he noted that China's aircraft are just one type of information node in a full detection system needed to protect China's airspace. To counter US air power, the Chinese claim their advanced air defense weapons, the S-300 and S-400 surface-to-air missile systems, along with a quantitative advantage in aircraft can defeat the US.[110] In addition, the Chinese are granting their pilots more autonomy than normally allowed to counter the US tactic of blinding and deafening the enemy. This doctrinal change of decentralized execution through greater autonomy created a change of authority in their air command and control. According to the 2006 White Paper on China's National Defense, "the Air Force has closed corps… and set up regional command posts"[111] now placing the "combat troops of the Air Force directly under the air commands of the military regions."

Since late 1999, the Chinese have discussed forming IW units either as a separate branch like the Army, Navy, and Air Force, or as independent departments within the Army. China's White Paper on Defense for 2006 mentions only information countermeasures units within the Army.[112] US defense analysts reported to Congress that "the People's Liberation Army has likely established IW units to develop viruses to attack enemy computer systems and networks, and tactics to protect friendly computer systems and networks."[113] Another report suggests that these units are not only capable of cyber and electronic attacks, they also have "anti-satellite

---

[110] Zhang Jian: "What's to Fear from the 'Raptor'?", Shanghai *Guoji Zhanwang* in Chinese 15 Oct 06. downloaded from www.opensource.gov in January 2007.

[111] Information Office of the State Council of the People's Republic of China, "China's National Defense in 2006", Beijing *Xinhua Domestic Service*, 29 Dec 2006. downloaded from www.opensource.gov CPP20061229704001 in January 2007.

[112] Information Office of the State Council of the People's Republic of China, "China's National Defense in 2006", Beijing *Xinhua Domestic Service*, 29 Dec 2006. downloaded from www.opensource.gov CPP20061229704001 in January 2007.

[113] Office of the Secretary of Defense (2005). "Annual Report to Congress: The Military Power of the People's Republic of China", p. 36. [electronic version]. http://www.defenselink.mil/news/Jul2005/d20050719china.pdf downloaded in October 2006.

capabilities aimed at countering US military technologies."[114] Along with cyber and IW units, the PLA remains committed toward increasing their IW infrastructure. The US-China Economic and Security Review Commission also stated the PLA now has their own IW schools and cyber-warfare regiments.[115] How these regiments fit within the military area commands is unknown.

However, the PLA continues to accelerate its informationization drive making it their second highest priority in the defense budget for 2006. Instead of a separate information warfare service, China's committed to digitizing its entire force and placing specialized IW teams within the PLA. These information specialists will not only come from the PLA but also from civilian institutions throughout China leveraging its main resource of 1.3 billion citizens.

This chapter examined how IO fits in China's strategic context, explained IO role in the PLA, and analyzed how IO affects their doctrine and organization. As such, China's military modernization focuses heavily on IW because Chinese IW provides the military new means of meeting China's national goals and IW, if properly executed, has proven an effective method of delaying air dominance. Russia has made similar observations regarding its use of IO in countering US air dominance.

[114] Josh Rosin, "China A Major Cyber Threat, Commission Warns", *Federal Computer Week*, 1 December 2006. [electronic version]. http://www.fcw.com/article96975-12-01-06-Web accessed in January 2007.

[115] Josh Rosin, "DoD: China Fielding Cyber-attack Units", *Federal Computer Week*, 25 May 2006. [electronic version]. http://www.fcw.com/article94650-05-25-06-Web accessed in January 2007.

CHAPTER FOUR

RUSSIA

IO and Russia's Military Modernization

Andrew Marshall summarizes the need for reviewing foreign lessons, specifically Russia's because their calculations are likely to make different assumptions about scenarios and objectives which often result in substantially different assessments from those of the US.[116] President Vladimir Putin announced in 2004 three national objectives for rebuilding Russia. By 2010, Putin's plans include doubling Russia's Gross Domestic Product, reducing its poverty, and modernizing Russia's military.[117] One key document that is shaping Russia's military reformation is a defense white paper drafted in 2003 by Sergei Ivanov, Russia's Minister of Defense, that describes Russia's view of modern warfare and outlines several important lessons from foreign military operations. This chapter outlines the role of IO in Russia's military modernization plan, examines Russia's view of IO as a means of countering US air dominance, and reviews how their doctrine and organizations have incorporated IO. The starting point for understanding how IO influenced Russia's military reformation begins with a look at Russia's National Security Concept because it lists foreign IO as a key threat to its national security.

Foreign information operations pose a significant threat to Russia's economic and military progress because of its growing dependency on information technology.[118] Russia

---

[116] Michael Pillsbury (2000). *China: Future Security Environment*. National Defense University: Washington DC. p. preface.

[117] The National Institute for Defense Studies (2004). "Russia—From Stability to Growth", *East Asian Review 2004*. The Japan Times, Ltd: Tokyo. p. 155. downloaded from http://www.nids.go.jp/english/dissemination/east-asian/pdf/east-asian_e2004_06.pdf in February 2007.

[118] Thomas Friedman defines a new international economic system—Globalization. This system has replaced the Cold War economy by flattening its structure through information technology. He states that Globalization is the integration of capital, technology, and information across national borders. In order for a nation's economy to grow, he posits that it must become globally connected to other world-wide markets.

believes that information warfare (IW) constitutes the most promising asymmetrical threat to developed nations because information vulnerabilities rise in direct proportion to a states' reliance on information.[119] Ivanov views modern warfare as highly asymmetric because instead of using traditional military force against military targets, modern warfare now engages military targets as well as nation's economic infrastructure with IO. Essentially, a key piece of Russia's military modernization relies on information technology to provide an asymmetric element of modern war. In addition, Russia's current military doctrine identifies IO as a means of countering military and non-military threats and also uses information technology to bridge its short-term, military modernization goals with its long-term, systemic changes.

Russia's current strategy for modernizing its military is a selective investment of key capabilities which were based on a careful analysis of their adversary's vulnerabilities.[120] Ivanov's defense white paper identifies key capabilities as precision strikes, air power, and information warfare which were all used to gain the initiative in war. Ivanov believes that outcomes in past wars were determined by its success in the initial phase and the party that takes the initiative early will achieve victory.[121] Ivanov's premise closely follows US Joint Publication 3-13 noting that gaining information superiority facilitates timely and accurate decision-making and maintains the initiative in war by operating inside an adversary's decision cycle. Given Russia's reduced defense budget, IW has become a cost-effective capability to counter the threats outlined in Russia's military doctrine.[122] Militarily, long-term, systemic changes are needed to not only maximize the effectiveness of IW but also to counter emerging threats such as the

---

[119] Mary C. Fitzgerald (2001). "Russian Military Policy and International Objectives: Interim Strategies and Plans for Long-Term Systemic Change", Hudson Institute: Washington DC, p. 10.

[120] Ibid. p. 7.

[121] Marcel de Haas, "Russia's Military Strategy: Preparing for the Wrong War", *Power and Interest News Report*, 24 April 2006. downloaded from http://www.clingendael.nl/publications/2006/20060424_cscp_online_dehaas.pdf in February 2007.

[122] Makhmut Gareev, "The Academy of Military Sciences in 2001 – 2005: Achievements and Problems", *Moscow Military Thought* 31 Mar 2006. [FBIS Translated Text CEP20060505466004].

growing lethality of precision air strikes. These systemic changes along with Ivanov's key capabilities are the core of what Major General Vladimir Slipchenko, former professor of strategy at the Russian Academy of Military Sciences, called non-contact or sixth generation warfare.

Slipchenko theorizes that warfare has progressed through five generations and is entering the sixth generation based on advances in information technology. He claims that "non-contact wars are waged…by basically inflicting precision strikes from afar through air and space."[123] This type of war is characterized by concealment, speed, accuracy, and a high degree of effectiveness through these strikes.[124] Russia's current military structure lacks the proper force distribution and technical basis for this type of warfare. Slipchenko advocated that Russia should not only prepare for an asymmetric, non-contact war, but also adopt an entirely different structure for its armed forces.[125] Justifying this he stated:

> "If today our armed forces function in three distinct mediums, air, sea and land, what we need is two functional branches: strategic attack and strategic defense forces. No tank armies will roll across the Russian border [because] future war will involve non-contact precision strikes against the state and military control systems, communications, and economy."[126]

Interestingly enough, Slipchenko does not include the information domain as one of the distinct mediums forces will operate in, yet non-contact warfare requires information superiority over an adversary. In this sense, he views air power as the dominating force in non-contact war because of its ability to deliver precision guided munitions. Since information superiority is a necessary

---

[123] Vladimir Slipchenko, "The Strategic Content of The State's Military Reform (A Prognostic View),"
Vooruzheniye. Politika. Konversiya, 7 July 2003. [FBIS Translated Text CEP20031229000123].

[124] Qiao Liang and Wang Xiangaui (1999). *Unrestricted Warfare*. PLA Literature and Arts Publishing House: Beijing, p. 49.

[125] Makhmut Gareev & Vladimir Slipchenko (2005). "Future War", Foreign Military Studies Institute; Leavenworth. p. 5.

[126] Ibid. p. 5.

piece of gaining air superiority, it can be inferred that IW is simply a component of non-contact war. So, what is Russian IW and how do they believe it counters US air dominance?

Russian Information Operations

Information war, according to Russia's Foreign Intelligence Service, is the established control over an adversary's information resources, deterring a potential adversary's development of information technology, disrupting an adversary's information networks and communication systems, and developing information weapons for safeguarding the security of a country's own information infrastructure and flow.[127] Colonel Mikhail Shutenko offers another definition claiming IW is an information competition aimed at creating informational and psychological effects on hostile countries' with the goal of influencing the decision-making process among adversary's highest-level military and political leaders. According to a report by Russia's Academy of Military Science, the main goal of IW is "the disintegration and destruction of the integrity of the enemy's command and control, breaking them into isolated, disoriented and uncontrollable elements and their subsequent removal from service by means of fire (physical) destruction."[128]

The definition offered by the Foreign Intelligence Service clearly focuses on controlling, deterring, and disrupting the information domain to protect their use of that medium. Shutenko's definition takes a more offensive approach and sets the framework for Russia's two categories of information war—information-technical and information-psychological. In truth, most Russian theorists believe IW contains both offensive and defensive forms that contribute to a war. They

[127] Unattributed interview with Vyacheslav Trubinkov. "SVR Chief Trubinkov Interviewed", Moscow *Nezavisimoye Voyennoye Obozreniye* in Russian 17 Jul 98. Downloaded from FBIS FTS19980728001250 in February 2007.

[128] [Unattributed author]. "Lessons and Conclusions from the War in Iraq", Russian Academy of Military Sciences. 11 Jul 2003. downloaded from FBIS report number CEP20030911000356 in February 2007.

also claim that the term "information war" does not fit since war, according to Russia's Academy of Military Science, is a socio-political phenomena and encompasses more than just one domain. Therefore, a more appropriate term for this type of operation is information confrontation which is similar to the US view of information operations. In short, Russia views information warfare as having information-technical and information-psychological components which are used to control the information domain just as the US Air Force would use its three components of IO to gain information superiority over an adversary. Denying an adversary information superiority is an important first step towards denying them air superiority.

Russia's Lessons from Operation Allied Force

Operation Allied Force and its use of air warfare, precision munitions, and information operations added a new dilemma to Russia's national security. Moscow believed "information warfare, precision strike weapons, and the US-NATO concern to reduce the risk of casualties would lead to a new form of contact-less warfare"[129] which reinforces Slipchenko's view of war. This type of non-contact war is one that Russia was not prepared to fight and certain adjustments were necessary. Russia's Minister of Defense Sergeyev echoed this view when he stated "the US demonstrated a significant military-technical breakaway in the sphere of information support of combat operations that must be countered."[130] According to Sergeyev, one clear lesson Russia learned from Allied Force is that disrupting an adversary's information resources through the use of information confrontation could delay air superiority.

This lesson fits well with the Russian view on the current Revolution in Military Affairs in that information technology enables greater precision. Greater precision allows for more

[129] Jacob Kipp, "Russia's Non-Strategic Nuclear Weapons", *Military Review*, May/June 2001. p. 30-31.

[130] Timothy Thomas, Foreign Military Studies Office, Fort Leavenworth, KS. "The Russian View of Information War", This article was first published in *The Russian Armed Forces at the Dawn of the Millennium*, 7-9 February 2000.

flexibility in targeting and theoretically, a faster and decisive victory. The targets that Lieutenant General Short wanted to strike, specifically those targets that would compel Milosevic to yield, were the exact types of targets Moscow believed to be the most effective use of precision air strikes and created the psychological impact necessary to win. Colonel Tsyganok, a Russian military analyst, reflected on the lessons of past 15 years of war and noted "the decisive factor was not the military defeat of the armed forces of the defending army, but the political isolation of its leaders."[131] The information-technical component of IW captures the level of precision that is necessary to not only isolate a leader but also target low observable or stealth aircraft which Serbia, with Russia's help, successfully accomplished in Allied Force. Therefore, it is mainly through the information-technical aspect of IW that Russia believes it can counter US air strikes.

Russia's Lessons from Operation Enduring Freedom

Operation Enduring Freedom demonstrated how synchronizing information-technical and information-psychological components of IW produced a faster and decisive victory. The use of Army Special Forces early in the campaign demonstrated the information-psychological element by uniting the Northern Alliance and building a Southern Alliance from scratch. Both alliances proved critical in toppling the Taliban. Precision air strikes against the Taliban's air defense systems and air power's supporting role in the ground offensive demonstrated the information-technical element. According to General Gareev, Enduring Freedom was a classic display of IW because it linked the use of non-lethal systems to incapacitate combat formations but did not affect the civilian population.[132] The result of synchronizing both components of IW was a clear information advantage for the coalition and was an essential piece of establishing air superiority.

[131] Colonel A. D. Tsyganok, "Lessons and Conclusions from the War in Iraq", Russian Academy of Military Sciences. 11 Jul 2003. downloaded from FBIS report number CEP20030911000356 in February 2007.

[132] S.A. Bogdanov. "The Probable Appearance of Future Warfare", Moscow: *Voyennaya Mysl*, 15 Dec 2003. downloaded from www.opensource.gov CEP20040115000246 in February 2007.

In the end, the alliance's ability to quickly destroy the Taliban's early warning systems as well as their command and control gave Russia much to think about.

If Slipchenko's view of future war is indeed correct, then precision air strikes against Russia's nuclear capabilities, command and control, and economic systems are vulnerable and accessible targets for the west. Countering these precision air strikes require the Russian's to gain the initiative through information operations. Like the US demonstrated during Operation Enduring Freedom, a strong information-technical component combined with the information-psychological element of IW denies an adversary a needed element of air superiority from which precision air strikes are generated. This premise was reinforced during Operation Iraqi Freedom and documented in an Academy of Military Science report on the lesson of the Iraq War in 2003.

Russia's Lessons from Operation Iraqi Freedom

Having analyzed US military operations in the Iraq theater since 1991, the Russians expected a similar display of military strategy from the 2003 Iraq War as Desert Storm. The Russian template for US military operations predicted air power to lead the with precision air strikes against Iraqi early warning radars, command and control nodes, air defense systems, and key elements of the Iraqi ground force followed by coalition ground troops to deliver the decisive blow. However the head of Russia's Academy of Military Science, General Gareev, believes victory was achieved "not so much by the quantity and quality of aerial attack weapons as much as by the complete informational superiority of US and British armed forces and its effective command and control."[133] The Academy developed a report on the lessons of the Iraq War and divided it into three informational phases that focused IW on strategic and operational objectives. According to the report, the first phase used information-psychological (propaganda) elements to

[133] M. A. Gareev, "The Academy of Military Sciences in 2001 – 2005: Achievements and Problems", *Moscow Military Thought* 31 Mar 2006. downloaded from www.opensource.gov, CEP20060505466004 in February 2007.

establish legitimacy and set the stage for subsequent military operations. The second phase continued emphasizing propaganda through mass media but also sought to demoralize the Iraqi leadership and began electronic warfare (information-technical) operations against key Iraqi nodes. The third phase was an unrestricted use of all elements of IW on Iraqi leadership and the people. The same report concludes that:

> "it was not the condition of the air force and air defense weaponry, nor the army's demoralization [as] the primary reasons for the lack of success of Iraq's air force and air defense combat operations [rather] it was through information operations aimed at the Iraqi command structure to believe it would be impossible to achieve even insignificant results by virtue of the complete superiority of the [coalition]."[134]

One possible reason that the information-psychological component was so effective stems from the fact that the US had conducted no-fly operations in northern and southern Iraq since 1991 reinforcing the message that Iraq would not be successful. Even though the Iraqi Air Force was no match against coalition air power, Russia did learn an important lesson from Iraq War in that a properly synchronized IO campaign can effectively delay an enemy's ability to achieve air superiority. Specifically, Russia can use IO to "drain sorties and munitions away from legitimate target sets, preserving them or providing the margin of survivability needed to accomplish their objectives."[135] This premise is based on Reflexive Control Theory which "creates a pattern or provides partial information to an enemy commander causing him to react in a pre-determined manner."[136] This underlying theory is the foundation of Russian information-psychological

---

[134] M. A. Gareev, "The Academy of Military Sciences in 2001 – 2005: Achievements and Problems", *Moscow Military Thought* 31 Mar 2006. downloaded from www.opensource.gov, CEP20060505466004 in February 2007.

[135] Michael O'Halloran, USMC. "A Kill is a Kill: Asymmetrically Attacking US Airpower", Air University: Maxwell. June 1999. p. 36.

[136] Timothy Thomas (2005). *Cyber Silhouettes: Shadows Over Information Operations*, Foreign Military Studies Office: Leavenworth. p. 241.

operations. These and other lessons noted by senior Russian military theorists in the Academy of Military Science, ultimately influenced Russia's military doctrine.

Information Operations in Russian Military Doctrine

In June 2005, President Putin charged military leaders with formulating a new military doctrine that focuses on the transformation of the armed forces, the development of an integrated air and space defense system, and the use of contact and non-contact methods of warfare.[137] Russia's military doctrine reflects "official ideas on military development and preparing its armed forces to defend the fatherland."[138] As such, their military doctrine outlines ways of conducting armed conflict to protect Russia's national interests. Currently, Russia's National Security Concept identifies their national interests and highlights foreign information operations as one of the key threats to their national security. In short, Russia's new military doctrine must reflect the military methods required to counter foreign IO and identifies information technology as a key enabler for transforming their military.

Using lessons from the 2003 Iraq war, Russian military theorists believe that information operations are a key component for adaptive air operations.[139] Their military doctrine discusses how information operations can deny air superiority to an adaptive enemy. These operations include securing information networks and the use of camouflage, concealment, deception and secrecy (operational security) to protect Russia's own information and confuse military decision

---

[137] Viktor Litovkin, "General Gareyev Says Russia Changing Its Military Doctrine", RIA Novosti, Moscow (RIA Novosti) Jan 18, 2007 http://www.spacewar.com/reports/General_Gareyev_Says_Russia_Changing_Its_Military_Doctrine_999.html accessed in February 2007.

[138] Viktor Litovkin, "General Gareyev Says Russia Changing Its Military Doctrine", RIA Novosti, Moscow (RIA Novosti) Jan 18, 2007 http://www.spacewar.com/reports/General_Gareyev_Says_Russia_Changing_Its_Military_Doctrine_999.html accessed in February 2007.

[139] "Lessons and Conclusions from the War in Iraq", Russian Academy of Military Sciences. 11 Jul 2003. downloaded from FBIS report number CEP20030911000356 accessed in February 2007.

makers planning adaptive air operations.[140] A Hudson Institute report on Russian military policy highlights an example of the military-technical nature of Russia's Military Doctrine noting the development of "information weapons to neutralize the most vulnerable components of Precision Guided Munitions."[141] The development of information weapons emphasizes the importance of information operations within national security as well as its role in countering air superiority. Russia's emphasis on information operations goes beyond military applications and is captured in Russia's Doctrine of the Information Security of the Russian Federation. This document has begun to change the organization of Russia's military.

Changes in Russian Military Organizations

"The key conclusion we must draw from the latest Gulf war is that the obsolete structure of the Russian armed forces has to be urgently changed."[142] In fact, the urgency to change their organization was building since Operation Allied Force in 1999. NATO's sole use of air strikes to compel an adversary was a wake-up call for Russia's National Defense. Militarily, the growth in information technology added new weapons and greater lethality to existing munitions while the commercial market used information technology to streamline communications which flatten and decentralized organizations. Russia's military organizational change incorporated elements of both sectors.

President Putin placed military organizational reform prior to 2010 as one of his top national goals. This reform calls for a reduction of troops, streamlining the services and military districts, and moving away from conscription and towards a contract-based military. Leveraging

[140] [unattributed author]. "Lessons and Conclusions from the War in Iraq", Russian Academy of Military Sciences. 11 Jul 2003. downloaded from FBIS report number CEP20030911000356 in February 2007.

[141] Mary C. Fitzgerald (2001). "Russian Military Policy and International Objectives: Interim Strategies and Plans for Long-Term Systemic Change", Hudson Institute: Washington DC, p. 12.

[142] Fred Weir, "Iraqi Defeat Jolts Russian Military," *Christian Science Monitor*, April 16, 2003, p. 6.

information technology to fewer troops reduces the cost of modernization and fulfills one of the lessons noted by the Academy of Military Sciences which is to better disseminate accurate and timely information down to the tactical level. Giving Russia's armed forces an information technology edge can streamline command and control, provide greater collection capability, and provides depth in counter-information operations. Specifically, the more information nodes that Russia can create (deception) adds more complexity for the US when conducting precision air strikes against key information nodes. Likewise, streamlining the services and military districts promotes decentralized execution and adds another dimension of complexity for achieving air superiority against Russia. Russia's military organizational reform capitalizes on information technology to facilitate decentralized execution, provide a better structure for conducting non-contact wars, and disseminate information faster than their opponent. These three components rely on the information domain and are exactly what Russia hopes to protect through the use of information operations. Finally, this type of structural reform makes it difficult for an adversary to gain and maintain air superiority.

This chapter examined the role of IO in Russia's military modernization plan, analyzed Russia's view of IO as a means of countering US air dominance, and reviewed how their doctrine and organizations incorporated IO. Russia's military modernization is a selective investment of key capabilities such as IO to fit within Russia's new paradigm of future warfare. As such, Russia believes that IO constitutes the most promising asymmetrical threat to developed nations because information vulnerabilities rise in direct proportion to a states' reliance on information. This theory, along with the observation that synchronizing technical and non-technical aspects of IO, was developed from Russia's observations of past US air campaigns. These and other lessons are captured in the next chapter.

CHAPTER FIVE

CONCLUSIONS

This monograph analyzed the question of what lessons, over the past ten years of US air operations, have foreign militaries integrated into their doctrine and organization to counter US air dominance. The air campaigns in Kosovo, Afghanistan, and Iraq provided the historical background for an analysis of both Chinese and Russian lessons learned. The lessons both countries identified and implemented show that IO was a key asymmetric capability that changed foreign military doctrine and organizations to counter US air dominance. Based on that premise, there are important conclusions concerning the conduct of IO in peace-time, the confusion surrounding IO terminology, the challenges of identifying deception in the targeting and operational analysis process, and the integration of IO and air superiority objectives.

While many different views of IO exist, each service still views IO only as a war-time operation leaving a gap in its peace-time application. The Russians observed that IO was a key factor toward gaining the initiative early in war and as such, their IO begins well before hostilities and provides an information preparation of the environment from the strategic to tactical level. For the US, the one office that could provide the information umbrella and synchronize strategic to tactical IO is the Office of Strategic Communications. Even though strategic communication is the overarching capability, the military component remains the most engaged to influence and shape conditions and must do more peace-time IO instead of focusing primarily on war-time aspects of IO. More peace-time IO engagement would do more to not only gain the initiative in war but also add legitimacy and support from partner nations.

Regarding IO terminology, a service or country's definition of IO reflects how it sees itself as decisive. Therefore, it is nearly impossible to build a common lexicon for IO since each

service or country views technology and to a lesser extent, the use of military force differently.[143] For example, China refers to IO as "information warfare" highlighting an offensive and defensive view of this medium while Russia calls IO "information confrontation" emphasizing an offensive mindset. However, both definitions as stated in chapters three and four reflect each country's strengths and philosophy of war. Similarly, the US Air Force and US Army definitions are different from the Joint definition of IO in that their related or supporting components are unique to each service. However, the focus of IO for all three is to influence decision-making while protecting our own information systems.

The Air Force must develop better counter-deception methodologies specifically within targeting and operational analysis. It is apparent that US adversaries will observe our actions and build a template of US operations and then devise a counter-strategy. Their counter-strategy will use some form of deception based on that template to lure the US into a position of disadvantage. As such, an adversary's use of IO, especially deception, can be an inexpensive method to counter air dominance by committing more US sorties against false targets. Simple deception techniques such as those used during the Kosovo Air Campaign are cheap and effective methods to drain sorties away from legitimate target sets. In addition, if countries like Russia can template an adversary's actions using pattern analysis, then deception operations combined with analysis have a greater probability of success. As such, more effort must be placed on determining the effects of air operations as well as identifying potential enemy deception operations.

Nesting both air and information superiority objectives from the strategic level down to the tactical level creates a synergy that is greater than the sum of their parts. As pointed out in the Iraqi Perspectives Project, the mixture of influence operations and precision air strikes is an extremely powerful combination for maximizing an effect and more emphasis should be placed

[143] Carl H. Builder (1989). *The Masks of War: American Military Styles in Strategy and Analysis*. Johns Hopkins Press: Baltimore. p. 12.

on influence operations throughout an entire air campaign. Even though the US's strength lies in its ability to create new, technical aspects of IO, countries like China emphasize the non-technical forms of IO like operational security, concealment, and deception as an asymmetric counter to the US's technical edge. Therefore the US must integrate the technical and non-technical aspects of IO such as precision strikes and influence operations to not only facilitate air superiority but also to simultaneously gain information superiority. As demonstrated during Operation Iraqi Freedom, influence operations can effectively bridge air and information superiority objectives. However, until an adversary can effectively interfere with the US's ability to gain and maintain information dominance, gaining air superiority will continue to be the main priority in modern war for the US Air Force.

BIBLIOGRAPHY

Arkin, William "Air head's: Misperceptions and rivalries obscure air power's potential". *Armed Forces Journal*. June 2006.

Biddle, Stephen "U.S. Military Operations in Iraq: Planning, Combat, and Occupation". John Hopkins University lecture series, Nov, 2005. http://www.sais-jhu.edu/merrillcenter/Panel1_Summary.pdf

Blank, Stephen (2006). "China's Military Power: Shadows Over Central Asia". The Lexington Institute: Arlington.

Bogdanov, S."The Probable Appearance of Future Warfare", Moscow: *Voyennaya Mysl*, 15 Dec 2003. downloaded from www.opensource.gov CEP20040115000246 on Jan 2007.

Boyne, Walter (2003). *Operation Iraqi Freedom: What Went Right, What Went Wrong and Why*. Tom Dougherty Associates: New York.

Builder, Carl H. (1989). *The Masks of War: American Military Styles in Strategy and Analysis*. Johns Hopkins Press: Baltimore.

Bush, George. "Address to the US" 7 (October 2001). [online version]. http://www.globalsecurity.org/military/library/news/2001/10/mil-011007-usia01.htm

Byman, D and Waxman, M. "Kosovo and the Great Air Power Debate". *International Security*, 24:4. MIT Press Journals.

Chuan, Pai "Command System of the Chinese Army", Hong Kong, *Ching Pao* No 257, 01 Dec 1998. [online]. Downloaded from www.opensource.gov, FTS19981212000281.on Dec 2006.

Chun-Shih, Hsien-Tai "China's Major General Wang Pufeng Discusses Definition, Significance of Information Warfare", *PRC Monthly Journal covering international and Chinese military affairs*. 11 April 2000. https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_246_203_0_43

Cordesman, Anthony (2002). *The Lessons of Afghanistan; War Fighting, Intelligence, and Force Transformation*. Center for Strategic and International Studies: Washington DC.

Cordesman, Anthony (2002). *The Lessons of Afghanistan; War Fighting, Intelligence, and Force Transformation*. Center for Strategic and International Studies: Washington DC.

Cordesman, Anthony (2003). *The Iraq War; Strategy, Tactics, and Military Lessons*. Center for Strategic and International Studies: Washington DC.

Corpus, Victor. "Part 1: Striking the US Where It Hurts", *Asia Times Online*. 18 Oct 2006. [electronic version: http://www.atimes.com/atimes/China/HJ19Ad01.html] downloaded on Feb 2007.

Creighton, J., et.al. (2004). "Effects Based Operations in Afghanistan; The CJTF-180 Method of Orchestrating Effects to Achieve Objectives". *Field Artillery Magazine,* Jan/Feb 2004.

de Haas, Marcel. "Russia's Military Strategy: Preparing for the Wrong War", *Power and Interest News Report*, 24 April 2006. [electronic version: http://www.clingendael.nl/publications/2006/20060424_cscp_online_dehaas.pdf]

Department of Defense, "Air Force Doctrine Document 2-5: Information Operations". 11 January 2005.

Department of Defense annual report to Congress: Military Power of the People's Republic of China. 2006.

Department of Defense, "Kosovo: Operation Allied Force After-Action Report". 31 Jan 2000. [electronic document: http://www.defenselink.mil/pubs/kaar02072000.pdf]

Department of Defense, "Multi-Service Concept for Irregular Warfare", 2 August 2006

Department of Defense (2006). "Military Power of the People's Republic of China". [electronic version: http://www.defenselink.mil/pubs/pdfs/China%20Report%202006.pdf]

Drew, D and Snow, D (1988). *Making Strategy: An Introduction to National Security Processes and Problems*, Air University Press: Montgomery.

Fitzgerald, Mary (2001). "Russian Military Policy and International Objectives: Interim Strategies and Plans for Long-Term Systemic Change", Hudson Institute: Washington DC.

Flanagan, S and Marti, M (2003). *The People's Liberation Army and China in Transition*. National Defense University Press: Washington DC.

Gaddis, John (2002). "National Security: On Strategic Surprise" [Electronic Version]. *Hoover Digest*. Spring, 2002 from http://www.hooverdigest.org/022/gaddis.html on Sep 2006.

Gaddis, John (2002). *The Landscape of History*. New York: Oxford University Press.

Gareev, Makhmut "The Academy of Military Sciences in 2001 – 2005: Achievements and Problems", *Moscow Military Thought* 31 Mar 2006. downloaded from www.opensource.gov, CEP20060505466004 on Jan 2007.

Gareev, M and Slipchenko, V (2005). "Future War", Foreign Military Studies Institute; Leavenworth.

Goldstein, Avery "Great Expectations: Interpreting China's Arrival". *International Security*. Vol 22, No. 3.

Hanlon, Michael E. (2002). "A Flawed Masterpiece". *Foreign Affairs Journal*, Vol 81, No. (3).

Horowitz, and Reiter (2001). "When Does Aerial Bombing Work? Quantitative Empirical Tests, 1917-1999". *The Journal of Conflict Resolution*, April 2001.

Hucheng, Wang "The US Military's 'Soft Ribs' and Strategic Weaknesses", *Liaowang*: Issue 27, 5 Jul 2000.

Information Office of the State Council of the People's Republic of China, "China's National Defense in 2006", Beijing *Xinhua Domestic Service*, 29 Dec 2006. downloaded from www.opensource.gov CPP20061229704001 on Jan 2007.

Jefferson, N. T. "Battlefield Exploitation". Department of Land Warfare on behalf of Joint Doctrine and Concepts Centre (Shrivenham, UK), dated 5 Nov 2000.

Jianlin, L and Meiquan, W. "PLA Prudently Discuss Joint tactical Corps", *Jiefangjun Bao* (Internet Version - WWW). 10 May 2005. downloaded from www.opensource.gov on Dec 2006.

Jian, Zhang "What's to Fear from the 'Raptor'?", Shanghai *Guoji Zhanwang* in Chinese 15 Oct 06. downloaded from www.opensource.gov on Dec 2006.

Johnson, David (2006). *Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post-Cold War Era*. RAND: Santa Monica.

Kipp, Jacob "Russia's Non-Strategic Nuclear Weapons", *Military Review*, May/June 2001.

Klimenko, A. "The Evolution of China's Military Policy and Military Doctrine", *Military Thought*, April-June 2005. [electronic version: http://www.findarticles.com/p/articles/mi_m0JAP/is_2_14/ai_n15623000/print]

Krepinevich, Andrew (2003). "Operation Iraqi Freedom: A First-Blush Assessment". Center for Strategic and Budgetary Assessments: Washington DC.

Lambeth, Benjamin (2005). *Air power against terror: America's conduct of Operation Enduring Freedom*. Santa Monica: RAND Corporation.

Lambeth, Benjamin (2001). *NATO's Air War for Kosovo; A Strategic and Operational Assessment*. Rand Project AIR FORCE: Santa Monica.

Lambeth, Benjamin "Lessons from the War in Kosovo". *Joint Force Quarterly*, Spring, 2002.

Liang, Q and Xiangaui, W (1999). *Unrestricted Warfare*. PLA Literature and Arts Publishing House: Beijing.

Litovkin, Viktor "General Gareyev Says Russia Changing Its Military Doctrine", *RIA Novosti*, Moscow (RIA Novosti) Jan 18, 2007 [electronic version: http://www.spacewar.com/reports/General_Gareyev_Says_Russia_Changing_Its_Military_Doctrine_999.html downloaded on Jan 2007]

Lyon, Charlie "Operation Allied Force: A lesson on Strategy, Risk, and Tactical Execution". *Comparative Strategy*, 2001.

NATO, "24 April Press Release". http://www.basicint.org/europe/NATO/99summit/10-13.htm

Ng, Ka Po (2005). *Interpreting China's Military Power: Doctrine Makes Readiness*. Frank Cass of Taylor & Francis: New York.

[No author provided]. "Taiwan Report on PRC Development on Laws of Armed Conflict", *Taiwan Defense Affairs*, 1 Sep 2004. [electronic version: www.opensource.gov] on Nov 2006.

O'Brien, Kevin, "Information Operations and the Kosovo Conflict", RAND Europe Senior Analyst. [electronic document: http://www.isodarco.it/courses/trento02/paper/trento02-brien_inf.pdf]

Office of the Secretary of Defense (2005). "Annual Report to Congress: The Military Power of the People's Republic of China", p. 36. [electronic version: http://www.defenselink.mil/news/Jul2005/d20050719china.pdf]

O'Halloran, Michael "A Kill is a Kill: Asymmetrically Attacking US Airpower", *School of Advanced Air and Space* Studies, Air University: Maxwell. June 1999.

Pillsbury, Michael (2000). *China: Future Security Environment*. National Defense University: Washington DC.

Qingmin, Dai (Major. General. PLAAF). "On Seizing Information Superiority", Beijing *Zhongguo Jungshi Kexue*, 20 April 2003. downloaded from www.opensource.gov, CPP20030728000209 on Nov 2006.

Rosin, Josh "China A Major Cyber Threat, Commission Warns", *Federal Computer Week*, 1 December 2006. [electronic version: http://www.fcw.com/article96975-12-01-06-Web]

Rosin, Josh "DoD: China Fielding Cyber-attack Units", *Federal Computer Week*, 25 May 2006. [electronic version: http://www.fcw.com/article94650-05-25-06-Web]

Segal, Adam (2002). *Digital Dragon. High Technology Enterprises in China*. Council on Foreign Relations: Cornell.

Singer, P.W. (2001). "Winning the War of Words: Information Operations in Afghanistan". Institute of Communication Studies, University of Leeds, United Kingdom.

Slipchenko, Vladimir "The Strategic Content of The State's Military Reform (A Prognostic View)," *Vooruzheniye. Politika. Konversiya*, 7 July 2003. [FBIS Translated Text CEP20031229000123].

The Hudson Institute (2005). "China's New Great Leap Forward: High-Tech and Military Power in the Next Half Century", Hudson Institute: Cicero.

The National Institute for Defense Studies (2004). "China-In Search of New Thinking", *East Asian Review 2004*. The Japan Times, Ltd: Tokyo.

The National Institute for Defense Studies (2004). "Russia—From Stability to Growth", *East Asian Review 2004*. The Japan Times, Ltd: Tokyo. Downloaded from http://www.nids.go.jp/english/dissemination/east-asian/pdf/east-asian_e2004_06.pdf on Oct 2006

Thomas, Timothy (2001). "China's Electronic Strategies". *Military Review*. May/June 2001 [electronic version: http://leav-www.army.mil/fmso/documents/china_electric/china_electric.htm]

Thomas, Timothy (2005). *Cyber Silhouettes: Shadows Over Information Operations.* Foreign Military Studies Office: Leavenworth.

Thomas, Timothy "The Russian View of Information War", Foreign Military Studies Office, Fort Leavenworth, KS. [This article was first published in *The Russian Armed Forces at the Dawn of the Millennium*, 7-9 February 2000.]

Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations*. 6th ed. Chicago: University of Chicago Press, 1996.

Tse-tung, Mao "On Protracted War," *Selected Military Writings of Mao Tse-tung* (Peking: Foreign Languages Press, 1968), [electronic version: http://www.marxists.org/reference/archive/mao/selected-works/volume-2/mswv2_09.htm]

Tsyganok, A (Colonel) "Lessons and Conclusions from the War in Iraq", Russian Academy of Military Sciences. 11 Jul 2003. downloaded from FBIS report number CEP20030911000356. on Jan 2007.

[unattributed]. "Operation Enduring Freedom-Afghanistan" [online version: http://www.globalsecurity.org/military/ops/enduring-freedom.htm]

US National Security Strategy 2006, http://www.whitehouse.gov/nsc/nss/2006/nss2006.pdf

USCENTAF, Assessment and Analysis Branch. "Operation Iraqi Freedom – By the Numbers". April 2003.

US Joint Forces Command, "Iraqi Perspectives Project".

[unattributed author]. “Lessons and Conclusions from the War in Iraq”, Russian Academy of Military Sciences. 11 Jul 2003. downloaded from FBIS report number CEP20030911000356.

[unattributed interview with Vyacheslav Trubinkov]. “SVR Chief Trubinkov Interviewed”, Moscow *Nezavisimoye Voyennoye Obozreniye* in Russian 17 Jul 98. Downloaded from FBIS FTS19980728001250 on Dec 2006.

Wang, Pufeng (Major General, PLA) (1995). “The Challenges of Information Warfare”. [electronic version]. http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm

Wang, Pufeng, (Major General, PLA). “China’s Major General Wang Pufeng Discusses Definition, Significance of Information Warfare”. *Hsien-Tai Chun-Shih*. 11 April 2000. downloaded from www.opensource.gov, CPP20000503000133 on Dec 2006.

Warden, John. “Air Theory for the Twenty-first Century”, *Aerospace Power Chronicles*, 1995.

Weir, Fred “Iraqi Defeat Jolts Russian Military,” *Christian Science Monitor*, April 16, 2003.

Xin, Tian “Effects of US War in Afghanistan on China’s Military Thinkers”, *Wen Wei Po*, 4 Feb 2002. downloaded from FBIS (www.opensource.gov) CPP20020204000032 on Oct 2006.

Yazhou, Liu (Lieutenant General, PLAAF) “China-America: The Great Game”, Eurasian *Review of Geopolitics*, Jan 2005.

Yoshihara, Toshi (2001). “Chinese Information Warfare: A Phantom Menace or Emerging Threat?”, Strategic Studies Institute: Carlisle.

Zhansan, Ke "Studies in Guiding Ideology of Information Operations in Joint Campaign", Beijing *Zhongguo Junshi Kexue*, 20 Apr 2003. downloaded from www.opensource.gov, CPP20030728000210 on Dec 2006.