

AIR WAR COLLEGE

AIR UNIVERSITY

IDENTIFYING AND DEFEATING INFILTRATION THREATS TO
THE HOMELAND

by

Michael T. Imbus, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

23 February 2007

[Cleared for public release 12/10/2007, AU 07-193]

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government and is not to be reproduced or published without the permission of the Air War College.

Contents

	<i>Page</i>
INTRODUCTION	1
LESSONS FROM HISTORY.....	4
German Sabotage Threats During World Wars I and II.....	5
Al Qaeda Strikes America	7
False Lessons from Operation IRAQI FREEDOM.....	8
EXAMINING ENEMY INFILTRATION AND SABOTAGE THREATS	10
Infiltration Methods.....	10
A Framework for Analyzing Foreign Infiltration Threats.....	13
ANALYZING THE INFILTRATION AND SABOTAGE THREATS POSED BY THE PEOPLE’S REPUBLIC OF CHINA	16
China’s Presence in the United States	17
PRC Intelligence Operations in the United States.....	20
Chinese Intelligence Collection Priorities	21
PRC Special Operations Capabilities	23
PRC Military Doctrine.....	26
Rating the Infiltration Threat Posed by China.....	29
ATTACK SCENARIOS	31
Attack Methods.....	32
Attacks on the Defense Transportation System.....	33
Attacks against Key Military Facilities and Leaders.....	36
Attacks Designed to Impact Morale	36
CI’S ROLE IN IDENTIFYING AND NEUTRALIZING INFILTRATION THREATS.....	38
Current US Counterintelligence Structure.....	38
DOD Counterintelligence Resource Shortfalls.....	42
DOD CI Structural Weaknesses	43
Current Laws and Directives that Impact DOD CI and Investigative Activities	44
Issues of Trust and Credibility.....	47
RECOMMENDATIONS AND CONCLUSIONS	51
Moving Beyond Terrorism to a Focus on Full-Spectrum Infiltration Threats	52
Meeting the CI Challenges of 21st Century	53

Improving the Connection Between DOD CI and the War Fighting Role of the COCOMs	56
Conclusion	59
BIBLIOGRAPHY.....	62

Chapter 1

Introduction

Although the United States has dedicated considerable effort and resources to countering terrorist threats to the Homeland, these measures have not addressed the full range of infiltration threats faced by the Nation. This paper explores the full spectrum of infiltration threats to the Homeland and examines the danger posed by foreign controlled or directed operatives who enter the United States for the purpose of conducting espionage, sabotage, assassination or terrorist attacks. Using historical examples, it demonstrates the likelihood enemy operatives could enter the United States undetected and conduct hostile acts.

Following this discussion, the paper proposes an analytical framework useful for examining the full range of infiltration threats posed by both state and non-state actors. This framework includes an adversary's presence in the United States and the ease at which their nationals can access US society, their ability and demonstrated intent to conduct aggressive and sophisticated intelligence operations within the United States, the collection priorities of their espionage operations, the special operations capabilities of their military and paramilitary forces, and the nature of their military doctrine and their focus on asymmetric operations. The applicability of this analytical framework is demonstrated via an examination of Chinese infiltration capabilities. This examination explores the likelihood China would have the ability and intent to conduct

terrorism, assassinations, sabotage attacks and espionage operations within the United States in the event of military conflict.

This paper also discusses the probable US targets enemy sabotage operatives would strike. It discusses four primary target categories including: 1) Strikes against critical military and civilian transportation infrastructure and assets required to deploy military forces; 2) Assaults against key military installations designed to destroy critical weapons systems and command and control nodes; 3) Assassinations of senior political and military leaders; and 4) Attacks designed to impact US morale.

Counterintelligence (CI) is one of the primary tools that can counter infiltration threats, but unfortunately the US Intelligence Community has generally treated CI as an adjunct requirement and failed to devote adequate attention and resources to this essential discipline. DOD CI is not immune from these problems, and currently suffers from resource shortfalls that impede its ability to properly counter the full range of infiltration threats to the Homeland. Despite the changes in the threat environment in the post Cold War and 9/11 era, DOD continues to focus the bulk of its intelligence efforts on foreign intelligence activities and devotes minimal resources to CI activities. This paper calls for a reevaluation of the balance between DOD foreign intelligence and CI resources.

In addition to resource shortfalls, DOD CI also suffers from structural weaknesses that separate Service CI activities from the war-fighting mission of the Combatant Commands (COCOMs). Although a recent US Government Commission recommended major changes in the organization and authority of DOD CI elements to address these structural weaknesses, this paper demonstrates that the linkage between Service CI activities and the COCOMs can be adequately strengthened by relying on existing DOD CI doctrine and directives. This approach

would capitalize on the existing COCOM authority over Service CI activities during wartime operations, and place certain DOD CI agents under the OPCON of USNORTHCOM. This solution would balance Service and COCOM CI needs, while granting USNORTHCOM direct control of CI activities supporting critical Homeland Defense activities.

By focusing analytical effort against the full range of infiltration threats, clarifying DOD's role in countering these threats, and better connecting DOD CI activities to the Homeland Defense mission of USNORTHCOM, DOD can improve its ability to counter infiltration threats and more effectively protect the Homeland.

Chapter 2

Lessons from History

The United States has faced threats from foreign infiltrators throughout the course of its history. Although the 9/11 attacks serve as the most prominent example of foreign directed sabotage or terrorism against the Homeland, these attacks were certainly not the first time enemy operatives targeted the United States. German operatives infiltrated the United States for the purpose of conducting sabotage attacks during both World Wars, and the fear of Japanese directed espionage and sabotage following the bombing of Pearl Harbor led President Roosevelt to order the internment of 117,000 Japanese Americans during World War II.¹ Unlike our World War II adversaries, the Iraqi government did not devote serious effort to conducting sabotage attacks against the US Homeland during Operations DESERT STORM or IRAQI FREEDOM. Iraq's failure to strike the United States can be tied to leadership, planning, and structural weaknesses within the Iraqi intelligence and military services. Unfortunately, future adversaries may not be challenged by the weaknesses that plagued Iraqi intelligence. These future adversaries may have both the intent and capability to conduct sabotage operations within the United States.

¹ Pierce O'Donnell, *In Time of War* (New York: The New Press, 2005), 48.

German Sabotage Threats During World Wars I and II

Germany mounted sabotage operations against the US Homeland during both World Wars. World War I German sabotage operations in the United States were managed by Germany's Military Attaché in Washington DC and a German Naval Intelligence Officer who infiltrated the United States using a fraudulent Swiss passport. These men recruited German merchant seamen and immigrants to help them conduct attacks. Significant incidents of suspected World War I German sabotage included the 1916 destruction of a thousand tons of munitions destined for Great Britain, France and Russia at the Black Tom pier in New York, and 1917 explosions at a Kingsland, New Jersey shell packing plant and the Hercules Gunpowder Company in Eddystone, Pennsylvania. From 1915 to early 1917, 43 American factories suffered fires or explosions of suspicious origin, and bombs were placed aboard four-dozen US merchant vessels carrying war supplies to the allied powers.² In addition to using explosives to conduct attacks, German agents also used biological agents to conduct sabotage in the United States and other areas. German agents infected horses shipped from the United States to Europe with glanders and anthrax bacteria in an attempt to damage allied logistics capabilities.³ The Nazis tried to repeat this pattern of sabotage during World War II.

In June 1942, eight Nazi operatives were tasked to enter the United States and destroy strategic transportation, manufacturing, and power generation facilities. These attacks were designed to cause panic, damage American morale, and prevent US industry from supplying war material to the allies.⁴ Hitler wanted to send waves of saboteurs to strike terror in the US

² Michael Warner, "The Kaiser Sows Destruction," *Studies in Intelligence* 46, no. 1 (2002) <https://www.cia.gov/csi/studies/vol46no1/index.html>.

³ Gavin Cameron, Jason Pate and Kathleen Vogel, "Planting Fear, How Real is the Threat of Agricultural Terrorism," *Bulletin of the Atomic Scientists* 57, no. 05 (2001) http://www.thebulletin.org/article.php?art_ofn=so01cameron.

⁴ O'Donnell, *In Time of War*, 21-22.

Homeland, and viewed this operation as the first wave of attacks. The German Abwehr recruited the operatives for this operation based on their English Language skills and prior long-term residence in the United States. The operatives did not possess advanced military training in commando operations nor did they have solid experience or skills in clandestine intelligence operations.⁵ The saboteurs, divided into two four man-man teams, traveled from France to US waters aboard German Navy U-Boats. Although both teams successfully entered the United States and melted into American society, their mission would ultimately end in failure.

The first team landed at Amagansett Beach near the tip of Long Island on 13 June 1942 and quickly encountered an unarmed US Coast Guard petty officer patrolling the beach. Although they were not immediately taken into custody, this incident prompted a search that discovered the weapons, explosives and uniforms the Germans had hidden on the beach. This discovery led to the initiation of a large Federal Bureau of Investigation (FBI) manhunt.⁶ The second group of Nazi operatives landed on 17 June 1942 at Ponte Vedra near Jacksonville Florida.⁷ Although they successfully entered the United States without detection, their ultimate fate was tied with that of their colleagues in New York.

The leader of the first group of Nazi operatives decided to approach the FBI to betray his mission and fellow saboteurs, and by 27 June 1942 all eight Nazi operatives were in FBI custody. In August 1942, a military tribunal convicted the eight Nazi saboteurs. Six of the men were executed, and the remaining two received long prison sentences.⁸ The failure of this mission convinced Hitler to abandon his plan to send waves of saboteurs to the United States.⁹

⁵ Ibid, 22-23, 87.

⁶ Ibid, 56-62, 67.

⁷ Ibid, 86.

⁸ Ibid, 78-85, 97

⁹ Ibid, 284.

Although the Nazis used a similar mode of operation to enable two espionage agents to enter the United States in November 1944, this mission also failed when one of these agents foiled the operation by turning himself and his fellow agent into the FBI.¹⁰ As demonstrated by the 9/11 attacks, it is unlikely that future enemy operatives will be so cooperative as to turn themselves in to US authorities before completing their assigned missions.

Al Qaeda Strikes America

The 11 September 2001 attacks graphically illustrated the damage terrorist infiltrators could cause to the US Homeland. Nineteen men, who were neither experienced intelligence operatives nor special operations professionals, were able to enter the United States and assimilate into US society without drawing the attention of US security officials. These men received training, financial, and logistic support from a transnational terrorist enterprise, but did not have the backing of a nation state. They traveled under their true names using legally acquired travel documents, and did not use sophisticated tradecraft.¹¹ The terrorists eventually seized four airliners armed with nothing but box cutters, and used these aircraft to strike at the symbols of US economic and military power.

Al Qaeda spent approximately \$400,000 - \$500,000 to conduct the 9/11 attacks.¹² This investment led to the deaths of 3,000 people, and resulted in \$27.2 billion in direct costs.¹³ This fact led the 9/11 Commission to state:

¹⁰ Ibid, 284-285.

¹¹ The National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, (Washington DC: Government Printing Office, 22 July 2004), 169,229, also available online at <http://www.9-11commission.gov/report/index.htm>.

¹² Ibid, 169.

¹³ Robert Looney, "Economic Costs to the United States Stemming from the 9/11 Attacks," *Center for Contemporary Conflict*, 5 August 2002, <http://www.ccc.nps.navy.mil/rsepResources/si/aug02/homeland.asp>.

The 9/11 attack was an event of surpassing disproportion. America had suffered surprise attacks before—Pearl Harbor is one well-known case, the 1950 Chinese attack in Korea another. But these were attacks by major powers.

While no means as threatening as Japan's act of war, the 9/11 attack was in some ways more devastating. It was carried by a tiny group of people, not enough to man a full platoon. Measured on a governmental scale, the resources behind it were trivial. The group itself was dispatched by an organization based in one of the poorest, most remote, and least industrialized countries on earth.¹⁴

Given the devastation resulting from these attacks, it is almost unimaginable to consider the damage a large enemy special operations contingent, thoroughly trained as elite, professional soldiers, armed with advanced weapons and backed by a robust intelligence collection capability could inflict on the United States.

False Lessons from Operation IRAQI FREEDOM

America's experiences during Operation IRAQI FREEDOM could lead American security officials to downplay the infiltration threat the United States may face in future conflicts. Iraq was a unique model. Saddled with incompetent leadership, a weak external intelligence apparatus, and little history of conducting successful special operations missions outside her borders, Iraqi operatives posed little threat to the US Homeland. The Iraqi Intelligence Service reflected the paranoia and internal security concerns of Saddam Hussein, and thus exerted little effort to develop and maintain an external network of assets capable of conducting sophisticated espionage and sabotage operations outside Iraq. Even after US forces entered Iraq, Saddam remained convinced that the primary threat to his regime was an uprising of Shiites in Southern Iraq or a military coup.¹⁵ This preoccupation with internal threats led Saddam to focus the external efforts of his intelligence service against Iraqi oppositionists living in the United States

¹⁴ The National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, 339-340.

¹⁵ Michael R. Gordon and Bernard E. Trainor, "Even as U.S. Invaded, Hussein Saw Iraqi Unrest as Top Threat," *New York Times*, 12 March 2006.

and other countries. Although Iraqi intelligence successfully recruited and managed a limited number of sources in the United States before the war, these agents were tasked to gather and report information on Iraqi dissidents.¹⁶

In addition to being saddled with poor leadership and a fixation on internal threats to the Hussein regime, Iraqi intelligence had little experience conducting successful sabotage or assassination operations outside their borders. The most famous Iraqi external operation conducted under the Saddam Hussein was the botched attempt to assassinate former President George H.W. Bush in Kuwait in April 1993. The Iraqi operatives tasked to conduct the assassination were quickly detected after they crossed the border, and Kuwaiti security officials eventually arrested 16 conspirators.¹⁷ During interrogations conducted by Kuwaiti security officials and the FBI, these operatives admitted they had received assistance from the Iraqi Intelligence Service.¹⁸

Although Saddam's forces were incapable of mounting sophisticated infiltration operations against the US Homeland, future adversaries may prove more adept. These future enemies will likely possess both the intent and capability to use sabotage and terrorism to strike directly at the Homeland. This potential threat makes it essential that US CI and security agencies be properly organized and equipped to detect and neutralize enemy sabotage operations.

¹⁶ Benjamin Weiser, "Another Son of Iraqi Ex-Diplomat Indicted," *New York Times*, 6 September 2003, Robert E. Pierre, "Editor Acted as Iraqi Agent, U.S. Charges," *Washington Post*, 10 July 2003, and "Iraqi Envoy's Son Charged," *Washington Post*, 15 April 2003.

¹⁷ Terrence P. Jeffrey, "How Saddam Tried to Kill Bush," *Human Events* 58, no. 36 (30 September 2002): 1,2.

¹⁸ Douglas Jehl, "Iraqi Tells FBI He Led Attempt to Kill Bush, US Officials Say," *New York Times*, 20 May 1993.

Chapter 3

Examining Enemy Infiltration and Sabotage Threats

Infiltration Methods

There are several ways potential adversaries could infiltrate intelligence operatives, terrorists or saboteurs into the United States. The first is to use diplomatic cover and place these operatives at their Embassy, Consulates, Interest Sections, Official Trade Offices and United Nations Permanent Missions in the United States. This method provides foreign operatives a legal, easy way to enter the United States and generally provides them diplomatic immunity if they are caught engaging in espionage or other intelligence activities. One drawback of using this method is the fact that each country has a finite number of diplomatic positions, thus limiting the number of operatives they can place in these positions. Another drawback is that placing an operative in the United States under diplomatic cover makes it impossible for them to mask their affiliation with a foreign government. This clear connection with a foreign government brings them to the attention of US CI officials and results in undesirable attention being paid to their activities.

In addition to using official cover positions, foreign operatives can use non-official cover to enter and operate within the United States. Foreign operatives can pose as students, businessmen, journalists, merchant mariners, airline crewmembers, or immigrants to enter the United States. As these operatives assimilate into American society, it becomes increasingly difficult to track them and detect their involvement in intelligence or sabotage activities. As

larger numbers of legal and illegal immigrants from a particular country or region enter the United States, individuals attract less attention and become more difficult to track and monitor. A drawback of non-official cover positions is that these operatives lack diplomatic immunity and are subject to arrest by US authorities if they are caught engaging in espionage or other illegal activities. The non-official cover status of these operatives also makes it more difficult for their country to control and communicate with them. On the positive side, operatives functioning under non-official cover are extremely difficult for US CI agencies to track and monitor. These operatives can literally melt into US society until activated by their government to conduct operations in the event of conflict or other crisis. In addition, the sponsor government can deny responsibility if these operatives are caught.

Finally, an adversary could use covert or clandestine means to penetrate US land borders or the US coast. The relative ease of unlawfully entering the United States has been aptly demonstrated during the ongoing debate over illegal immigration. It is estimated there are seven to 20 million illegal immigrants currently residing in the United States.¹⁹ The inability to arrive at a consensus regarding the actual number of illegal immigrants in the United States helps illustrate the difficulty of determining the actual national security threat posed by illegal immigration. Although it is feasible terrorists or hostile SOF operators could use traditional narcotic or human smuggling methods and routes to infiltrate the United States, accurately quantifying this threat is difficult. Despite the difficulty of accurately quantifying the threat posed by enemy operatives illegally entering the Homeland, the fact that 7 to 20 million largely unskilled immigrants have been able to successfully enter the United States leads one to

¹⁹ Brad Knickerbocker, "Illegal Immigrants in the US: How Many are There?," *The Christian Science Monitor*, 16 May 2006 <http://www.csmonitor.com/2006/0516/p01s02-ussc.htm>.

conclude that a trained, professional operative should have little difficulty exploiting this infiltration method.

The scope of the problem is at least partially illustrated by geography, and the vast number of illegal immigrants entering the United States every year. US Customs and Border Protection (CBP) is responsible for protecting the 5,000 mile border between the US and Canada, the 1,900 mile border between the US and Mexico, and over 95,000 miles of shoreline. In fiscal year 2006, CBP apprehended approximately 1.3 million illegal immigrants in the United States with 1.1 million of these individuals arrested between legal ports of entry.²⁰ During fiscal year 2005 CBP apprehended 1.2 illegal immigrants in the United States. 165,000 of these individuals were from countries other than Mexico, and 650 were from special interest countries.²¹

The primary drawback to using clandestine means to infiltrate the United States is found in the fact that CBP arrests over a million illegal immigrants every year. Any enemy operative who lacked the legal protection granted by diplomatic immunity or a valid US visa would face the risk of arrest and interrogation. Linking with human or narcotics smugglers to infiltrate operatives into the United States would also expose an adversary to the danger these criminals could intentionally or unintentionally compromise the operation. On the positive side, an operative who successfully infiltrated the United States using clandestine means would have no apparent affiliation with a foreign government. This lack of apparent government affiliation would give an adversary at least some degree of plausible deniability if they chose to use clandestine operatives to strike the United States.

²⁰ US Customs and Border Protection, *Performance and Accountability Report, Fiscal Year 2006*, (Washington, DC: 15 November 2006), 6.

²¹ Sara A. Carter, "Of Special Interest: U.S. Agencies Missing Links Between Illegal Immigration And Terrorism," *San Bernardino Sun*, 29 December 2006, http://www.sbsun.com/news/cj_4917538.

A Framework for Analyzing Foreign Infiltration Threats

DOD has long had a framework for analyzing terrorist threat levels in foreign countries that host US forces or serve as transit points. This framework quantifies the terrorist threat in a given country as: NEGLIGIBLE, LOW, MEDIUM, HIGH OR CRITICAL. This framework considers a minimum of five factors including: terrorist group existence, capability, history, trends, and targeting to determine the terrorist threat level in a given country.²² In the post-9/11 environment, Americans have become familiar with the color-coded Homeland Security Advisory System threat scale used by the Department of Homeland Security (DHS) to promulgate the terrorist threat to the US Homeland. Homeland Security Presidential Directive-3 instituted this five-level scale in March 2002.²³ Although both of these frameworks provide useful information, they focus exclusively on terrorism conducted by non-state actors and thus ignore the threat posed by espionage, sabotage, or assassination operations conducted by foreign nations using operatives capable of infiltrating the United States. This paper seeks to augment the existing DHS and DOD terrorist assessment tools by introducing an analytical framework for examining the full range of foreign infiltration threats.

Determining the infiltration threat to the United States posed by potential adversaries requires the examination of several factors. First, you have to determine the adversary's current official and unofficial presence in the country and their ease of access to the US Homeland. Does the country maintain diplomatic facilities such as an embassy, consulates, or trade offices in the United States or other countries in the Western Hemisphere? Do they send large numbers of students to study at US universities or colleges? Do they have a robust merchant marine or

²² Joint Publication 1.02, *DOD Dictionary of Military and Associated Terms*, 8 August 2006, <http://www.dtic.mil/doctrine/jel/doddict/>

²³ Homeland Security Presidential Directive-3, 11 March 2002.

national airline that allows their nationals to routinely operate at important US airports and seaports? Do they send business, trade or scientific delegations to the United States?

Next, you have to study the intelligence capabilities of the potential adversary. Have they demonstrated the ability to conduct sophisticated espionage operations against the United States? Do their external intelligence services maintain a paramilitary capability? What is the relationship between the intelligence service and military special operations forces? Do they work together to conduct reconnaissance, gather intelligence, and covertly infiltrate operatives into targeted areas or are they stifled by rivalry and distrust?

Third, studying a potential adversary's intelligence collection priorities can also provide insight into their future plans. A country that devotes considerable effort to monitoring its own nationals or dissidents abroad reflects a focus on internal security, and likely poses little direct espionage or sabotage threat to the United States. A country that focuses on collecting intelligence related to military capabilities, plans and intentions is probably doing so for conventional military and defense purposes. Collecting data on advanced science and technology programs allows a country to build its own capabilities without paying high research and development costs, and gathering data on advanced weapons systems can enable an adversary to develop tactics, techniques and procedures to defeat these weapons. Collecting political intelligence can improve a country's ability to meet its goals and objectives during international negotiations. On the other hand, a country that devotes a significant percentage of its intelligence collection efforts to gathering data on key landmarks in the United States, vital defense installations, critical transportation infrastructure, and large population centers may be collecting targeting data. Since few countries possess the capability to strike at the US

Homeland with conventional military forces, this intelligence could be used to support contingency planning for sabotage, assassination or terrorist attacks.

Unfortunately, determining foreign intelligence collection priorities is complicated by the fact the United States will never hold perfect knowledge of an adversary's intelligence activity. Intelligence collection is a clandestine activity, and intelligence operatives go to great lengths to mask their endeavors. CI professionals operate in an ambiguous world where things are not always what they appear. For this reason, US CI agencies must constantly ask themselves a fundamental question: Is country X's apparent lack of interest in a particular category of collection targets a reflection of reality, or is it merely a result of the US CI Community's inability to penetrate the foreign service and ascertain their true intentions?

Finally, you have to examine the potential adversary's military doctrine and the capabilities of their special operations forces (SOF). Does the country's military doctrine stress asymmetrical attacks against strategic targets in the enemy's rear area? Do they maintain SOF units capable of covertly infiltrating a target area and successfully striking key command and control facilities, transportation nodes used to deploy military forces, or essential military installations? Have they carried out successful sabotage operations in the past? Does the country maintain ongoing relationships with international terrorist organizations that could augment their SOF capabilities by acting as proxies to conduct attacks against the United States?

The analytical framework presented in this chapter offers a tool for examining the full range of infiltration threats to the Homeland. It is applicable to any state actor, and with slight modification can be used to evaluate the infiltration threat posed by a non-state entity such as a transnational terrorist organization.

Chapter 4

Analyzing the Infiltration and Sabotage Threats Posed by the People's Republic of China

To demonstrate the utility of the analytical framework presented in the previous chapter, it is helpful to apply it to a potential adversary. China is used for illustrative purposes based on a number of factors. First, as recognized by the February 2006 Quadrennial Defense Review, China is the most likely member of the international community to emerge as the next peer or near-peer competitor of the United States.²⁴ Secondly, China maintains a robust diplomatic presence in the United States, and the increasing economic ties between the two countries provide Chinese businessmen, merchant mariners, and students regular and routine access to the US Homeland. Third, China continues to conduct aggressive intelligence collection operations against the United States, and enhance the capability of its military special operations forces.²⁵ Finally, recent Chinese military doctrine and thought has stressed the concept of using asymmetric attacks to defeat a stronger enemy, and raised the idea of unrestricted warfare that does not differentiate between military and non-military targets.²⁶

²⁴ Department of Defense, *Quadrennial Defense Review Report*, (Washington DC: Department of Defense, 6 February 2006), 29.

²⁵ For information on Chinese espionage activities against the United States see: Director of Federal Bureau of Investigation and Director of Central Intelligence Agency, "Report to Congress on Chinese Espionage Activities Against the United States," (Washington DC, 1999), For information on the growing role of Chinese Special Operations Forces see: Scott J. Henderson, "In the Shadow: Chinese Special Forces Build a 21st Century Fighting Force," *Special Warfare* 19, no. 4 (July/August 2006): 30-35.

²⁶ For a full discussion of the concept of Unrestricted Warfare see: Colonel Qiao Lang and Colonel Wang Xiangsui, *Unrestricted Warfare; China's Master Plan to Destroy America* (Panama City, Panama: Pan American Publishing Company, 2002).

Although this paper applies this analytical framework to the People's Republic of China, a few caveats are in order. The first caveat is that although China is used to illustrate the merits of this analytical framework this paper does not address the likelihood of military conflict between the United States and China. Numerous scholars and policy makers have already provided differing perspectives on the threat a rising China will eventually pose to the United States.²⁷ This paper focuses on the likelihood China (or another possible adversary) would have the capability and intent to conduct or sponsor sabotage, assassination or terrorist attacks in the United States if war were to occur.

The second caveat is that although China is used to explain and demonstrate the analytical framework presented, this should not be construed to imply China poses the most likely sabotage or terrorism threat to the United States. A solid argument can be made that a weaker adversary such as North Korea or Iran, especially given their SOF capabilities and history of supporting terrorism, would be more likely to conduct sabotage attacks against the US Homeland in the event of military hostilities. A peer or near-peer competitor such as a future China may not pose the most likely sabotage threat to the US Homeland, but given their large presence in the United States and existing intelligence and SOF capabilities they likely pose the most dangerous sabotage threat to the US Homeland. DOD efforts to counter or minimize this threat would have applicability across the spectrum of potential adversaries.

China's Presence in the United States

The first step in evaluating the infiltration threat posed by a particular nation state is to examine that country's presence in the United States. China maintains an embassy in

²⁷ For an example of the conflicting opinions on the potential threat posed by China see: John J. Mearsheimer, "China's Unpeaceful Rise," *Current History* 105, no. 690 (April 2006), 160-162 and Zheng Bijian, "China's Peaceful Rise and Asia's New Role," Beijing: Xuexi Shibao, 2 May 2005.

Washington DC, and consulates in San Francisco, Los Angeles, New York, Houston, and Chicago.²⁸ In addition to these establishments, the PRC maintains a Permanent Mission to the United Nations in New York.²⁹ This robust official presence provides the PRC ample opportunity to infiltrate intelligence personnel into the United States. There are approximately 1,500 PRC diplomats and official commercial representatives living and working in the United States.³⁰ Stanislav Lunev, a former Soviet military intelligence officer who was previously assigned to Beijing and who defected to the United States in 1992, estimates that two-thirds of all permanent Chinese diplomatic positions in foreign countries are filled by intelligence personnel.³¹ If these figures are accurate, at any given time the PRC has 1,000 trained, professional intelligence personnel operating in the United States under official cover.

In addition to the personnel who staff PRC embassies, consulates and other official establishments, China can potentially capitalize on the large number of Chinese students who attend US universities and colleges. The Institute of International Education reported there were 62,523 Chinese students studying in the United States during the 2004-2005 academic year.³² Although it is unrealistic to expect that all or even a majority of these students are actually professional intelligence agents or sabotage operatives, this large pool of potential recruits provides China an incredibly valuable tool for gathering basic intelligence within the United States. The existing presence of large numbers of Chinese students could also allow China to

²⁸ Department of State, *Foreign Consular Offices in the United States Spring/Summer 2006*, (Washington DC: Superintendent of Documents, US Government Printing Office, 4 August 2006), 19-23.

²⁹ Permanent Mission of the People's Republic of China to the United Nations, <http://www.china-un.org/eng/>.

³⁰ Nicholas Eftimiades, *Chinese Intelligence Operations*, (Annapolis, MD: Naval Institute Press, 1994), 27.

³¹ Stanislav Lunev, "China's Intelligence Machine (Overseas Intelligence Activities)", *Insight on the News*, 13 no.42 (Nov 17, 1997).

³² Institute of International Education, "U.S. Sees Slowing Decline in International Student Enrollment in 2004/2005," <http://opendoors.iienetwork.org/?p=69736> (accessed 19 October 2006).

infiltrate large numbers of operatives into the United States without drawing undue attention from US CI and security agencies.

Growing trade between China and the United States has resulted in numerous Chinese companies operating in the United States. Based on the nature of the Chinese political and economic system, it is difficult to separate these companies from the Chinese government. The China Ocean Shipping Company (COSCO), one of the world's largest maritime shipping businesses, provides an example of Chinese state-owned commercial activity in the United States. COSCO vessels make routine visits to US seaports, including some of the strategic locations used to deploy US military forces in time of crisis. According to the Federal Maritime Commission, COSCO maintains a fleet of more than 600 ships that call at 1,100 ports in 150 countries. COSCO uses 59 transportation hubs in North America and makes weekly calls at the ports of Baltimore, New York, Charleston, Houston, Long Beach, Seattle, Oakland, and Norfolk.³³ The scope of Chinese shipping activity at these ports is illustrated by the fact China is the single-largest trading partner at the Port of Seattle, and approximately 8.8 billion dollars in bilateral trade passed through the port in 2003.³⁴ According to Senator James Inhofe, COSCO is owned by the Chinese People's Liberation Army and functions as the merchant marine of the Chinese military.³⁵ Air China, the flag airline of the Peoples Republic of China, provides passenger and cargo service between China and several US cities. Air China passenger and cargo flights routinely travel to Los Angeles, San Francisco and New York. In addition to these

³³ Federal Maritime Commission, "China Ocean Shipping Company," <http://www.fmc.gov/reading/ChinaOceanShippingCompany.asp> (accessed 1 November 2006).

³⁴ U.S. China Economic and Security Review Commission, *2005 Report to Congress of the U.S. China Economic and Security Review Commission*, 109th Cong., 1st sess, November 2005, 35.

³⁵ Timothy W. Maier, "China's Military May Get US Base," *Insight on the News* 15, no. 18 (17 May 1999): 14.

locations, Air China offers cargo service to Chicago and Portland.³⁶ These facts clearly demonstrate China has multiple channels for easy access to the United States.

PRC Intelligence Operations in the United States

According to the FBI, China currently poses a more significant intelligence collection threat to the United States than any other country.³⁷ China's primary civilian intelligence agency is the Ministry of State Security (MSS). The MSS was established in 1983, and holds responsibilities for collecting intelligence within foreign countries and conducting CI activities in China and abroad.³⁸ In addition to the MSS, China also maintains a military intelligence collection capability. The Military Intelligence Department of the Peoples Liberation Army General Staff is responsible for collecting foreign intelligence and military and technological information.³⁹

Chinese intelligence agencies have demonstrated the ability to use both official and nonofficial cover positions to allow their case officers to operate outside China's borders.⁴⁰ This ability allows them to capitalize not only on the Chinese diplomats and military attachés working in the United States and official delegations visiting the country, but also exploit the Chinese students, businessmen, journalists, merchant seaman, and scientists who visit the United States. In a joint FBI and CIA report to Congress, US CI officials highlighted China's history of using Chinese students to gather intelligence information, and pointed out China's use of its growing commercial presence in the United States to enhance its intelligence collection capabilities.⁴¹ It

³⁶ Air China, "English Language Homepage," <http://www.airchina.com.cn/index.jsp> (Accessed 1 November 2006).

³⁷ Peter Brookes, "The Spies Among Us," *The Heritage Foundation*, 1 June 2006, <http://www.heritage.org/Press/Commentary/ed060106c.cfm>.

³⁸ Eftimiades, *Chinese Intelligence Operations*, 17-19 and Director of Federal Bureau of Investigation and Director of Central Intelligence Agency, "Report to Congress," 2.

³⁹ Director of Federal Bureau of Investigation and Director of Central Intelligence Agency, "Report to Congress", 2.

⁴⁰ Eftimiades, *Chinese Intelligence Operations*, 21.

⁴¹ Director of Federal Bureau of Investigation and Director of Central Intelligence Agency, "Report to Congress", 1,3.

is estimated that there are over 3,000 Chinese front companies conducting espionage activities in the United States.⁴²

Although capable of mounting sophisticated, clandestine collection operations against the United States, Chinese agents frequently exploit information legally available from Western publications, US university libraries, unclassified databases, US research institutions, and the Internet.⁴³ In addition to traditional human intelligence collection operations, China is suspected of conducting aggressive computer network operations in an effort to obtain sensitive information. Chinese hackers have reportedly penetrated sensitive DOD and other US Government information systems, as well as US government contractor systems. In addition to allowing China to obtain large amounts of sensitive data, this effort could provide Chinese information warfare specialists background information that would allow them to degrade, shut down or exploit US computer systems during a crisis.⁴⁴ Besides these computer related capabilities, China operates communication intelligence collection systems directed at the United States from facilities located at Lourdes, Cuba.⁴⁵

Chinese Intelligence Collection Priorities

China devotes significant effort to gathering a broad spectrum of intelligence information from the United States. China is keenly interested in gathering science and technology information to advance her growing economy, and seeks political intelligence on US foreign

⁴² Peter Brookes, "Legion of Amateurs: How China Spies," *The Heritage Foundation*, 31 May 2005 <http://www.heritage.org/Press/Commentary/ed053105c.cfm> and Larry M. Wortzel, Ph. D, "Risks and Opportunities of a Rising China" (lecture, Conference on The Asian Century for Business: A Security Challenge, Washington DC, 23 May 2006) <http://www.heritage.org/Research/AsiaandthePacific/hl948.cfm>.

⁴³ Director of Federal Bureau of Investigation and Director of Central Intelligence Agency, "Report to Congress", 2-4.

⁴⁴ Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)," *Time*, 29 August 2005, <http://www.time.com/time/magazine/article/0,9171,1098961-1,00.html>.

⁴⁵ Lawrence G. Mrozinski et al, "Countering China's Threat to the Western Hemisphere," *International Journal of Intelligence and Counterintelligence* 15, no. 2 (Summer 2002): 195-210.

policy developments and intentions.⁴⁶ In addition, Chinese leaders recognize US military superiority, and seek to obtain US military and military related technology. Chinese intelligence operations have successfully obtained information on advanced US thermonuclear warheads, space and missile technology to include advanced guidance systems, high-powered computers, advanced machine tools, and jet engines. Further complicating the negative consequences of this espionage activity, China is suspected of providing advanced military technology to potential US adversaries including Iran and North Korea.⁴⁷

There is no publicly available information that indicates Chinese agents have been detected gathering information on the physical attributes and security of US military and other government facilities, population centers, communication nodes, transportation infrastructure, and other likely sabotage targets. Instead of indicating a lack of Chinese interest in these types of targets, this could simply mean China is using less-risky, legal methods to gather this type of data. As an open society, a great deal of information on US installations, transportation facilities, and key landmarks is publicly available. China has no need to send trained intelligence professionals to gather this type of data when it can be easily trained by an open source intelligence specialist via an internet connection in Shanghai, or collected by a merchant seaman or commercial airline pilot who visits these facilities in the course of his normal duties. The sheer number of Chinese diplomatic personnel, students, and business officials living in and visiting the United States makes it impossible for US CI agencies to monitor their activities. Reviewing other nations' foreign collection efforts illustrates the importance of monitoring Chinese and other foreign nationals residing in the United States.

⁴⁶ Director of Federal Bureau of Investigation and Director of Central Intelligence Agency, "Report to Congress", 1-2.

⁴⁷ House, *Report of the Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China*, 105th Cong., 2d sess., 1999, Report 105-851, ii, xii, xxix, xxxvi-xxxvii, 84-86, 123-130.

During the late 1990s and early 2000s, US CI professionals caught personnel assigned to Iranian Mission to the United Nations conducting apparent photographic and video surveillance of key landmarks and transportation infrastructure in New York including the Statue of Liberty, Rockefeller Center, the Brooklyn Bridge, the Queens-Midtown Tunnel, a subway station, the Staten Island Ferry Terminal, and Metropolitan Transit Authority buses.⁴⁸ Other than the UN Mission, the only Iranian diplomatic facility in the United States is a small Iranian Interest Section located in the Pakistani Embassy.⁴⁹ The small number of Iranian diplomats in the United States makes it relatively easy for US CI to track and monitor them. Iran's identification as a member of the "Axis of Evil", and the country's history of sponsoring terrorist attacks against US interests likely makes Iranian diplomats a primary focus of the FBI and other US CI agencies. Unlike their Iranian counterparts, Chinese intelligence officers and agents operating in the United States do not face this same level of scrutiny. They could theoretically collect data on potential sabotage targets while avoiding detection.

PRC Special Operations Capabilities

The Chinese military has a limited history of maintaining dedicated SOF units, and has no recent history of conducting complex sabotage and assassination operations outside China's borders. Additionally, China is not considered a state sponsor of terrorism and there is no information to indicate Chinese intelligence or SOF personnel maintain ongoing relationships with terrorist organizations.⁵⁰ The Peoples Liberation Army (PLA) fielded its first dedicated

⁴⁸ Peter Brookes, "Spooks, Lies and Videotape," *The Heritage Foundation*, 6 July 2004, <http://www.heritage.org/Press/Commentary/ed070604a.cfm>.

⁴⁹ Department of State, *Foreign Consular Offices*, viii.

⁵⁰ For details of China's counterterrorism efforts and information on state sponsors of terrorism see: Department of State, *Country Reports on Terrorism 2005* (Washington DC: Department of State Office of the Coordinator for Counterterrorism, April 2006), 66-67 and 171-177.

SOF unit in 1988.⁵¹ At the current time, each of the seven PLA military regions possesses regiment-sized SOF units.⁵² In his book, *Interpreting China's Military Power*, Ko Po Ng states Chinese SOF “are mainly trained in special reconnaissance, sabotage assaults, infiltration, guerrilla warfare, psychological operations and information operations.” Ng goes on to state these forces could be used to “attack enemy C4ISR centers and seize key air- and seaports.”⁵³ Other authors have stressed that PLA SOF focus on conducting direct action and special reconnaissance missions.⁵⁴ The bulk of Chinese SOF operators are assigned to the PLA, but the PLA Marine Corps and PLA Air Force Airborne Corps also maintain special operations units. There are currently 25,000 SOF operators in the Chinese Army and another 1,500 in the PLA Marine Corps. In addition, the PLA Air Force Airborne Corps maintain an unknown number of SOF battalions comprised of 400-500 operators.⁵⁵

As a comparison, the United States military has approximately 34,000 active duty SOF operators with an additional 15,000 assigned to the reserve components. In addition to these military forces, the Central Intelligence Agency (CIA) reportedly maintains a force of 150 SOF operators in its Special Activities Division.⁵⁶ North Korea maintains what arguably constitutes the largest Special Forces contingent in the world. Experts currently estimate that the North Korean People's Army has over 100,000 SOF operators. These SOF personnel are augmented

⁵¹ Xavier Gerard Smith, “Special Operations Forces in the People's Liberation Army and the Development of an Integral Unconventional Warfare Mission,” (Master's Thesis, Naval Postgraduate School, June 2005), 28.

⁵² Ka Po Ng, *Interpreting China's Military Power* (New York: Frank Cass, 2005), 128 and Smith, “Special Operations Forces,” 36.

⁵³ Ng, *Interpreting China's Military Power*, 128.

⁵⁴ Henderson, “In the Shadow:,” 30-35 and Smith, “Special Operations Forces,” 37.

⁵⁵ Smith, “Special Operations Forces,” 36-39.

⁵⁶ Andrew Feickert, *US Special Operations Forces (SOF): Background and Issues for Congress* (Washington, DC: Congressional Research Service, 28 September 2004), 1, 6..

by large numbers of special operations trained personnel assigned to North Korean intelligence agencies.⁵⁷

Although Iran maintains relatively small numbers of dedicated SOF, Iran's active support of and relationships with key terrorist organizations provide the country an impressive asymmetric capability. The United States Government currently identifies Iran as the international community's most active state sponsor of terrorism.⁵⁸ The Iranian army has one SOF division comprised of approximately 5,000 men, and the Iranian Revolutionary Guards Corps (IRGC) or Pasdaran also maintains a 5,000-man SOF division. The IRGC Quds Force augments these forces. Although the size and budget of the IRGC Quds Force is unknown, they are known to operate from Iranian diplomatic facilities located in foreign countries.⁵⁹ The IRGC serves as the primary Iranian Government interface with terrorist organizations such as Hezbollah and Hamas, and Iran relies on these organizations to conduct sabotage and terrorist actions on behalf of the regime.⁶⁰

Chinese SOF lacks the long history and full capabilities of their American counterparts, lacks the numbers of SOF operators fielded by the North Korean People's Army, and lacks the long-term connection with terrorist proxies enjoyed by the Iranian IRGC. Despite these facts, China has taken steps to enhance the SOF competencies of her military forces, and invested some of her best men and most advanced equipment to develop and field SOF capabilities.⁶¹ For these reasons, it would be a mistake for US defense officials to ignore Chinese SOF threats. China's growing SOF capabilities, coupled with her existing intelligence capabilities and robust

⁵⁷ Joseph S. Bermudez Jr., *North Korean Special Forces*, 2nd ed. (Annapolis, MD: Naval Institute Press, 1998), 1-3.

⁵⁸ Department of State, *Country Reports on Terrorism 2005*, 173.

⁵⁹ Anthony H. Cordesman, *Iran's Developing Military Capabilities* (Washington, DC: Center for Strategic and International Studies, 2005), 19, 46, 48-49.

⁶⁰ Ilan Berman, *Tehran Rising* (Lanham, MD: Rowman & Littlefield Publishers, Inc., 2005), 47.

⁶¹ Henderson, "In the Shadow."

presence in the United States provides her the basic capabilities needed to conduct sabotage strikes or assassination operations within the US Homeland. To determine the likelihood China would use these capabilities in a conflict with the United States, it is important to examine Chinese military doctrine.

PRC Military Doctrine

In addition to developing enhanced SOF capabilities, Chinese military professionals have developed doctrine that highlights traditional SOF missions and strengths. The study of foreign military doctrine is important in that it helps us determine what a country “can and probably will do” in the event of hostilities.⁶² Reviewing the military doctrine of a potential adversary is key to determining the likelihood they would conduct sabotage or support terrorist attacks in the United States.

As China’s economic strength and role in the international community has grown, her military leaders have sought to develop and adopt a military doctrine that reflects her status in the current international security order. Early Chinese Communist military doctrine stressed the strengths provided by China’s territorial size and large population. The People’s War concept of Maoist China emphasized “mass and defense in depth” while sacrificing “operational readiness for structural readiness.”⁶³ Chinese defense leaders have steadily moved from this defensive doctrine. Early Chinese defense policies and military doctrine focused exclusively on ensuring the survival of the PRC and maintaining its territorial integrity. Expanded national interests did not become an influence on Chinese military thought until the 1980’s. Chinese national interests now include not only the preservation of Chinese sovereignty and territorial integrity, but also

⁶² Ng, *Interpreting China’s Military Power*, 14.

⁶³ *Ibid*, 12.

ensuring the stability of the international order, maintaining and strengthening China's role in foreign affairs, safeguarding economic interests, expanding export markets, and maintaining access to overseas resources. As China has increased the external dimensions of its national interests, it has been forced to reexamine its security posture.⁶⁴

Chinese military doctrine is generally viewed as evolving through four phases. These phases include the People's War, People's War under modern conditions, local/limited war and local/limited war under high-technology conditions.⁶⁵ Three constants have survived the refinement of Chinese military doctrine from 1949 to present. The first constant is the preeminent position of PLA land forces in the Chinese military. Even today, the PLA Naval and Air Forces play a supporting role to their counterparts in the PLA land forces, and serve as their "junior partners".⁶⁶ The second is the long-term Chinese attraction to using asymmetric capabilities to target enemy weaknesses or to turn an enemy's strength against itself.⁶⁷ Finally, Chinese leaders have consistently viewed the United States as a potential threat.

Following the end of the Cold War, Deng Xiaoping stated Western countries had initiated a Third World War "without the smoke of gunpowder" aimed at "the peaceful evolution of socialist countries". Deng's views were supported and expanded on by a 1996 editorial published in an official Chinese Communist Party periodical. This editorial stated "The Westernization and splintering directed at China by Western Countries led by the United States will not change and the powerful, united conspirators will not relinquish their plot to contain China's development... They are plotting to destroy China as a fortress of socialism and

⁶⁴ Ibid, 25-27.

⁶⁵ Ibid, 39.

⁶⁶ Paul H.B. Godwin, "PLA Doctrine and Strategy: Mutual Apprehension in Sino-American Military Planning," in *The People's Liberation Army and China in Transition*, ed. Stephen J. Flanagan and Michael E. Marti (Washington DC: National Defense University Press, 2005), 267.

⁶⁷ Ng, *Interpreting China's Military Power*, 14 and J. Michael Waller, "PLA Revises the Art of War," *Insight on the News* 16, no. 8 (28 February 2000): 21.

subjugate China in an inferior position.”⁶⁸ In an article entitled “The PLA in a Changing China: An Overview,” Stephen J. Flanagan and Michael E. Marti state, “The PLA military strategy sees the United States as its principal adversary. As a result, the PLA increasingly emphasizes preemptive, asymmetric strikes against critical American military targets, as well as active and passive defenses against U.S. long-range precision strike systems.”⁶⁹

Chinese military officers have produced books and articles expounding on the use of preemptive and asymmetric attacks to defeat stronger adversaries. Although these works may not reflect official Chinese military doctrine, the fact they were published under the auspices of the PLA reflects that Chinese military officials believe they hold at least some degree of merit. In February 1996, Lu Linzhi published an article in the *Jiefangjun Bao* or *Liberation Army Daily* calling on Chinese military leaders to launch preemptive strikes in the event war with a stronger power becomes inevitable. Although Lu does not specifically identify the United States as the focus of his effort, it is easy to conclude from the context of the article that the United States is in fact the potential enemy referenced in his work. Lu praises the success of the Israeli forces in the 1967 six-day war, and faults Saddam Hussein for failing to seize the initiative in the first Gulf War by not conducting a preemptive strike against US forces. Lu recognizes that the United States “is most vulnerable during the early phase of the war when it is still deploying troops and making operational preparations.” Lu states this is the point China should launch an overwhelming strike using “fire assaults, special operations, and sabotage operations.” Lu writes that in determining the targets for these strikes, Chinese forces “should zero in on the hubs and other crucial links in the system that moves enemy troops as well as the war making machine,

⁶⁸ Ng, *Interpreting China’s Military Power*, 9.

⁶⁹ Stephen J. Flanagan and Michael E. Marti, “The PLA in a Changing China: An Overview,” in *The People’s Liberation Army and China in Transition*, ed. Stephen J. Flanagan and Michael E. Marti (Washington DC: National Defense University Press, 2005), 5.

such as harbors, airports, means of transportation, battlefield installations, and the communications, command and control, and information systems.”⁷⁰

Colonels Qiao Liang and Wang Xiangsui created a stir with the 1999 publication of their book *Unrestricted Warfare*. When interviewed by a reporter from the Chinese Communist Party youth league, Colonel Qiao stated, “The first rule of unrestricted warfare is that there are no rules, with nothing forbidden.”⁷¹ Unrestricted warfare transcends the boundaries between the worlds of war and non-war, and does not differentiate between military and non-military targets. The concept of unrestricted warfare stresses the use of asymmetric methods to “find and exploit an enemy’s soft spots.” The proponent of unrestricted warfare should strike where his “adversary does not expect to be hit” and should focus attacks on locations that “will result in a huge psychological shock to the adversary.” Colonels Qiao and Wang state the US military is ill-prepared to confront an enemy who engages in unrestricted warfare because US defense officials “have never taken into consideration and have even refused to consider means that are contrary to tradition and to select measures of operation other than military means.”⁷²

Rating the Infiltration Threat Posed by China

Using the analytical framework presented in this paper and information available from open sources, it is possible to evaluate and rate the infiltration threat China could pose to the US Homeland in the event of hostilities. For illustration purposes, the familiar five-tier scale of the current DOD terrorism matrix that characterizes terrorist threats as NEGLIGIBLE, LOW, MEDIUM, HIGH OR CRITICAL can be used to describe infiltration threats. The large number of Chinese citizens living, working, and studying in the United States would lead to a “HIGH”

⁷⁰ Lu Linzhi, “Preemptive Strikes Crucial in Limited High Tech Wars,” *Jiefangjun Bao*, February 14, 1996

⁷¹ Waller, “PLA Revises the Art of War,” 21-22.

⁷² Lang and Xiangsui, *Unrestricted Warfare*.”

rating in the Presence category. This rating reflects the reasonable assumption that clandestine Chinese intelligence agents and operatives are already present in the United States. China's demonstrated ability to conduct sophisticated clandestine intelligence operations and her current status as the single greatest espionage threat to the United States would result in a "CRITICAL" rating in the area of Intelligence Operations. On the other hand, the fact Chinese intelligence agencies do not currently focus their collection efforts towards gaining information that would allow them to plan sabotage, assassination or terrorism operations would result in a "LOW" rating in the area of Intelligence Collection Priorities. China's growing SOF capabilities provide a pool of highly trained operatives able to covertly operate within US borders to conduct sabotage and other direct action missions. Despite this fact, China lacks a long-term history of conducting successful SOF strikes outside her borders and lacks access to terrorist proxies to augment her SOF capabilities. For this reason, they would receive a "MEDIUM" rating in the SOF Capabilities category. Finally, China's emerging military thought stressing unrestricted warfare and the importance of conducting preemptive, asymmetrical strikes against a stronger enemy would lead to a "CRITICAL" rating in the Military Doctrine category. Consolidating these separate categories would result in an overall infiltration threat rating of "HIGH". Having developed a method for evaluating infiltration threats, it is important to examine the potential targets enemy saboteurs could strike.

Chapter 5

Attack Scenarios

In 2004, the US Army hired the RAND Corporation to examine the capabilities and tactics that would be required to maintain the US military's capability to counter enemy anti-access strategies and maintain access to key strategic regions. The scenarios in this study included US actions against a Saddam led Iraq, China, and Russia. In each case, the study discounted the enemy sabotage threat to the Homeland. The study found that sabotage strikes against aerial ports and seaports of embarkation "would be unlikely to have a direct military effect" and pose only "tertiary level threats" through 2012. The study further claimed, "The direct effects of such operations are likely to be minor because U.S. forces frequently train for this sort of contingency."⁷³ This RAND study failed to address the ease at which potential adversaries could infiltrate operatives into the United States, and the significant destruction or disruption these operatives could cause to militarily significant targets. The RAND study was also overly optimistic in its assessment that current US military training has prepared US forces to counter, or recover from such attacks. US adversaries could use a variety of methods to strike a broad range of targets in the Homeland in an effort to mitigate US military strengths and negatively impact US morale. Potential targets include the transportation infrastructure and assets used to

⁷³ Eric V. Larson et al., *Assuring Access in Key Strategic Regions* (Santa Monica, CA: Rand Corporation, 2004), 30-31, 52-53, 74-75.

deploy US military forces, key military installations and communications nodes, important military leaders, and targets specifically chosen to impact US morale.

Attack Methods

The bombing of the Murrah Federal Building in Oklahoma City, the Khobar Towers Attack in Saudi Arabia and insurgent attacks in Iraq have proven the effectiveness of vehicle borne improvised explosive devices. 9/11 showed how an attacker could use common items as weapons to achieve devastating effects. The March 1995 sarin gas attacks against Tokyo subway commuters, the fall 2001 anthrax attacks, and the November 2006 polonium-210 poisoning of Alexander Litvinenko have shown the ability of terrorists, criminals, or enemy agents to use chemical, biological, and radiological weapons to conduct sabotage attacks. These attacks caused fatalities, but their real power lay in the ability to cause fear and panic, force the evacuation of facilities, cause at least the temporary loss of equipment and resources, and require governments to commit time, effort, and financial resources to complex clean-up operations.

The fall 2001 anthrax attacks provide a solid example of the impact of a biological incident. The attack killed five people, and made 17 additional people ill. The US Postal Service estimated it spent \$1 billion responding to the attacks.⁷⁴ A letter containing anthrax spores was opened in the Hart Senate Office Building on 15 October 2001. Following this event, most House and Senate office buildings were closed for six to 19 days, approximately 6,000 people were tested for exposure to anthrax, 28 of these individuals tested positive for exposure, and roughly 1,000 people were placed on antibiotics as a precautionary measure.⁷⁵ The Hart Senate Office Building remained closed for three months following this incident and the Environmental

⁷⁴ “The Overlooked Attack,” *Washington Post*, 12 July 2005.

⁷⁵ S. Res. 187, 107th Cong., 1st sess., 2001.

Protection Agency estimated it spent more than \$14 million to decontaminate the building.⁷⁶ Following disclosures Mr. Litvinenko had been poisoned in London, thousands of people contacted the United Kingdom National Health Service based on fear they had also been exposed to polonium-201.⁷⁷ Although it is too early at this point to determine the full impact of the Litvinenko case, it is likely to have a major impact on the government and citizens of the United Kingdom.

Attacks on the Defense Transportation System

The US military relies on a combination of military and civilian transportation assets to deploy forces. The US Transportation Command (USTRANSCOM) relies on commercial transportation providers to meet 88 percent of continental US land transportation requirements, 50 percent of airlift needs, and 64 percent of global sealift requirements.⁷⁸ In general, US military personnel are moved from the United States to foreign areas by a combination of military and civilian airlift assets while heavy equipment and ammunition are moved via military and civilian sealift resources. It is estimated that in the event of a large-scale deployment, DOD would move approximately 95 percent of required equipment and supplies via sealift.⁷⁹ During a contingency, military forces would travel from major installations to the strategic seaports aboard military and commercial truck and civilian rail carriers using US highways and rail lines.

To meet its sealift requirements, DOD has identified 17 commercial facilities as strategic seaports. These strategic seaports would to be used to move military equipment in the event of

⁷⁶ Craig Gilbert, "Hart Senate Office Building Reopens," *Milwaukee Journal Sentinel*, 23 January 2002.

⁷⁷ Richard Beeston and Daniel McGrory, "Poison Plotters Claim Their Second Victim," *Times Online*, 2 December 2006 <http://www.timesonline.co.uk/article/0,,2-2482990,00.html>.

⁷⁸ United States Transportation Command, "About USTRANSCOM," <http://www.transcom.mil/organization.cfm> (accessed 23 November 2006).

⁷⁹ General Accounting Office, *Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployments Through Domestic Seaports* (Washington, DC: General Accounting Office, October 2002), 1.

crisis. Current strategic seaports include: Anchorage, Oakland, Long Beach, Port Hueneme, San Diego, Corpus Christi, Beaumont, Wilmington, Morehead City, Tacoma, Jacksonville, Savannah, Charleston, Philadelphia, Hampton Roads area Ports in Virginia, and the New York/New Jersey Port Complex.⁸⁰ As commercial facilities, these strategic seaports generally lack the military security found at DOD installations. DOD, commercial port operators, the US Coast Guard, and local, state and federal civilian law enforcement agencies share security responsibilities for military activities at strategic seaports. Foreign flagged and crewed vessels frequently operate in the same strategic seaports used for military movements.⁸¹

Examining sealift operations during previous conflicts helps illustrate the criticality of small numbers of US seaports. Eighteen military and commercial seaports in the United States and Puerto Rico were used to ship a total of 4,236,172 tons of cargo to the Middle East during Desert Shield and Desert Storm. Although 18 ports were used, four commercial seaports (Jacksonville, FL, Houston, TX, Bayonne, NJ, and Beaumont, TX) handled over 57 percent of the sealift cargo during this operation. Twenty one percent of Desert Shield and Desert Storm cargo moved from the Port of Jacksonville, and 18 percent moved from the Port of Houston.⁸² A successful Iraqi sabotage attack at the Ports of Jacksonville or Houston would have severely hampered US mobility operations. Although military shipments could have theoretically been shifted to other ports following an attack, this action would have complicated and slowed the deployment of forces to Southwest Asia.

⁸⁰ Patti Bielling, "Anchorage is Named DOD's Newest Strategic Seaport," *Military Surface Deployment and Distribution Command Public Affairs Release*, 17 August 2004.

⁸¹ The author served as the senior counterintelligence officer on the USTRANSCOM staff from August 2003-June 2006. In this capacity, he was responsible for coordinating military and civilian CI and criminal investigative support for US military transportation activities at US and foreign seaports. Fulfilling this role required an understanding of the security structure at the ports as well as maintaining awareness of foreign owned and crewed vessels utilizing the ports.

⁸² Douglas Menarchik, *Powerlift—Getting to Desert Storm* (Westport, CT: Praeger Publishers, 1993), 113.

Potential adversaries likely recognize the difficulty of securing in-transit military assets, and realize DOD personnel and equipment are most vulnerable while moving from secured DOD installations to contingency theaters. Sabotage strikes against military forces and equipment in transit, key transportation facilities, and the military and civilian transportation assets used to move military forces and equipment could significantly disrupt and delay deployment operations. Given DOD's heavy reliance on commercial seaports for the deployment of military equipment and the relatively small numbers of strategic ports identified for military use, in the event of crisis, enemy strikes against these ports could have a substantial impact.

The fact that these ports are also used to transport commercial goods coming to and from worldwide ports and frequently host foreign flagged and foreign crewed vessels presents serious vulnerabilities. These vulnerabilities would make it relatively easy for an adversary to collect intelligence on military activities at the port, security procedures, and critical port infrastructure. Foreign access to US strategic seaports could also provide a means for introducing enemy operatives. An enemy could conduct sabotage attacks against key US seaports in coordination with efforts to destroy or degrade allied ports in theater, the mining of important foreign harbors to prevent over-the-shore cargo discharge operations, and efforts to interdict the flow of US logistics in critical sea-lanes.⁸³ Coupled with computer network attack operations against the key information systems used to provide in-transit visibility of military equipment, these attacks could seriously degrade US power projection capabilities.

⁸³ Scott W. Conrad, *Moving the Force: Desert Storm and Beyond* (Washington, DC: Institute for National Strategic Studies, 1994), 51-52.

Attacks against Key Military Facilities and Leaders

Enemy sabotage attacks against key military facilities would serve the dual purpose of damaging or destroying critical weapons systems and making it difficult to command and control forces. The access control and security measures present at most military facilities would make these targets more challenging to strike than unsecured portions of the Defense Transportation System. Early attacks on military installations housing critical assets like the B-2 Bombers at Whiteman AFB, MO or the naval combatants at San Diego or Norfolk Naval Bases could prove devastating to US war plans especially if saboteurs were able to destroy or seriously damage aircraft or warships. Attacks against relevant Combatant Command (COCOM) Headquarters such as the US Pacific Command at Camp Smith, HI or US Central Command at MacDill Air Force Base, FL could hamper US ability to wage a major combat operation in their geographic area of responsibility. Assassinations of multiple military and civilian leaders would not only damage command and control, but also force the adoption of stringent personal protective measures that would restrict freedom of movement, divert security resources, and hamper efficiency.

Attacks Designed to Impact Morale

In addition to using sabotage attacks to strike at militarily significant targets, an enemy could also use threats and sabotage attacks to damage military and civilian morale. One scenario would be to conduct limited attacks at or near mission support areas at US military installations including family housing areas, medical facilities, childcare facilities, and commissaries. These attacks could be followed up by an information operations campaign directed against deployed military members highlighting the military's inability to protect their family members in the United States. The Internet makes it relatively easy to find personal information on military

members including home addresses, phone numbers, and e-mail addresses. How would the average deployed military member react to a threatening e-mail that included their home address, information on the school their children attend and a description of the vehicle their spouse drives? Given the information available via the Internet and the public domain, an enemy could gather this type of data with little difficulty.

Although this chapter has provided examples of targets enemy operatives could strike in the United States, in reality potential targets are only limited by the capabilities and imagination of the enemy. Enemy saboteurs could significantly damage critical defense infrastructure in the United States, negatively impact the US Military's ability to deploy and control forces, and potentially damage military morale. For this reason, it is important to explore the United States' capability to detect enemy operatives, prevent sabotage and assassination attacks, and respond to and recover from successful strikes on key infrastructure and facilities. CI is one of the essential tools DOD should emphasize in its effort to improve the department's ability to detect and neutralize infiltration threats.

Chapter 6

CI's Role in Identifying and Neutralizing Infiltration Threats

Any effort to examine DOD's current ability to identify and neutralize infiltration threats to the Homeland and develop recommendations to improve this ability must include a detailed examination of DOD CI. In order to examine CI, you must understand the distinction between CI and foreign intelligence. Executive Order 12333, *United States Intelligence Activities*, defines CI as, "Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities." In contrast, foreign intelligence is defined as "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities."⁸⁴ DOD organizations conduct both CI and foreign intelligence activities.

Current US Counterintelligence Structure

DOD is only one of the federal government organizations that hold CI responsibilities. The National Counterintelligence Executive (NCIX), an organization under the direct control of the Director of National Intelligence (DNI), is tasked to lead US CI efforts. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction

⁸⁴ Executive Order 12333, *United States Intelligence Activities*, 4 December 1981, Section 3.4.

(commonly known as the WMD Commission) found that NCIX lacks adequate budgetary authority or operational control over the activities of the various US Government agencies that hold CI authorities and responsibilities. In addition to DOD, both the FBI and CIA hold responsibilities for conducting CI investigations and operations. The FBI is the lead US domestic CI organization, and the CIA bears primary responsibility for conducting CI activities outside US borders.⁸⁵

Besides functioning as the lead US Government agency for CI in the United States, the FBI also serves as the lead agency for counterterrorism activities in the Homeland. To meet the expanded need for inter-agency coordination on counterterrorism activities in the post 9/11 era, the FBI has increased the numbers of Joint Terrorism Task Forces (JTTFs) operating in the United States. There are currently 101 FBI led JTTFs operating in cities throughout the United States. These task forces combine the talents of FBI special agent and analytical personnel, representatives from other federal law enforcement, intelligence and CI agencies, and state and local law enforcement professionals to fight terrorism.⁸⁶ DOD has detailed both CI and criminal investigative special agents to the majority of these task forces. These DOD agents currently report to their Service or agency chain of command while detailed to the JTTFs.

The FBI has historically separated the activities of agents involved in counterterrorism investigations from those involved in CI activities. This separation is reflected in the current “terrorism only” focus of the JTTFs. This separation hampers the overall effectiveness of FBI efforts to counter infiltration threats, and is especially damaging to countering the efforts of state

⁸⁵ The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington DC: The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 31 March 2005), 489-490 also available at <http://www.wmd.gov/report/index.html>.

⁸⁶ Robert S. Mueller III, Director, Federal Bureau of Investigation (Statement Before the House Appropriations Subcommittees on Science, Justice and Commerce, and Related Agencies, 14 September 2006) <http://www.fbi.gov/congress/congress06/mueller091406.htm>.

sponsors of terrorism who rely on their intelligence agencies to provide training, equipment, and other support to terrorist organizations. The FBI has sought to improve the synergy between counterterrorism and CI by placing both disciplines under a National Security Branch formed in September 2005.⁸⁷

Although a number of organizations in DOD conduct or support CI activities, the Services and the Counterintelligence Field Activity (CIFA) hold the majority of DOD CI authorities and responsibilities. The Service CI agencies including the Air Force Office of Special Investigations (AFOSI), the Naval Criminal Investigative Service (NCIS), and US Army CI are the only agencies in DOD with the charter and authority to conduct full-spectrum CI activities including collections, operations, and investigations. These organizations are under the command and control of the Military Department Secretaries to allow them to meet their Title 10 responsibilities.⁸⁸ CIFA holds the authority to represent DOD during consultations with NCIX, plays a key role in DOD CI budget and resource allocation decisions, holds broad CI program oversight responsibilities, and conducts DOD-wide CI training activities. Despite these authorities, CIFA lacks the authority to conduct CI collections, operations, or investigations.⁸⁹

In addition to holding full-spectrum CI responsibilities, AFOSI and NCIS are also responsible for conducting criminal investigative activities. Unlike the Navy and Air Force, the Army separates responsibility for CI and criminal investigations activities. The US Army Criminal Investigations Command (USACIDC) performs the criminal investigative mission

⁸⁷ Ibid

⁸⁸ DOD Directive 5240.2, *DOD Counterintelligence*, 22 May 1997, 3,7,14.

⁸⁹ The Commission on the Intelligence Capabilities of the US, *Report to the President*, 494, and DOD Directive 5105.67, *Department of Defense Counterintelligence Field Activity*, 19 February 2002.

within the US Army, and is also responsible for specific logistical security (LOGSEC) activities.⁹⁰

The COCOMs hold little direct authority over DOD CI activities. Each COCOM has a CI Staff Officer (CISO) tasked with coordinating CI support to the COCOM, and maintaining oversight of Service CI activities directly impacting the COCOM and its area of responsibility or performance of its functional mission. A Service CI agency is assigned executive agent responsibilities and holds primary responsibility for providing operational CI support to the COCOM. For Example, AFOSI is assigned executive agent responsibilities to support USNORTHCOM.⁹¹ CISOs lack authorities to conduct CI collections, operations, and investigations, and do not normally have operational control (OPCON) over Service CI elements supporting the command. The only time a COCOM holds OPCON over the activities of Service CI personnel is during the National Command Authority directed execution of an operational plan or operations order that specifies that Service CI elements will be placed under the control of the joint force commander. During these circumstances, the Service CI elements supporting the joint force commander fall under the command authority of the COCOM commander. Even then, the joint force commander only holds OPCON over CI collections and certain CI operations. The law enforcement and CI investigative activities undertaken by these forces remain under the control of the appropriate Service Secretary.⁹²

This complicated and confusing span of control makes it very difficult for the COCOMs to compel DOD CI activities to meet their requirements. The USNORTHCOM area of

⁹⁰ US Army Criminal Investigations Command, "US Army Criminal Investigations Command Mission," <http://www.cid.army.mil/mission.htm> (accessed 20 January 2007).

⁹¹ DOD Instruction 5240.10, *Counterintelligence Support to the Combatant Commands and the Defense Agencies*, 14 May 2004, 7, 15.

⁹² DOD Directive 5240.2, *DOD Counterintelligence*, 22 May 1997, 3.

responsibility provides an illuminating example of this frustration. Although USNORTHCOM holds primary responsibility for Homeland Defense activities and holds important force protection and defense critical infrastructure protection responsibilities, the command has no direct control over the Service CI activities that support these missions. This results in a situation where the USNORTHCOM CISO holds “asking” authority over the Service CI elements. USNORTHCOM can ask a Service CI element to provide support or conduct a particular operation or investigation, but they have no authority to set Service CI agency priorities or compel the accomplishment of a requested task.

DOD Counterintelligence Resource Shortfalls

The WMD Commission described US CI efforts as “fractured, myopic, and only marginally effective.” This commission went on to state that CI has been “treated as a second class citizen” in the intelligence profession, and remains “largely neglected” by policy makers and the intelligence community.⁹³ Although the US intelligence budget is classified, it is widely estimated the US spends approximately \$40 billion per year on intelligence.⁹⁴ Roughly 80 percent of the US intelligence budget is allocated to DOD, but only a small percentage of this funding is expended to finance CI activities.⁹⁵

A comparison between the personnel assets allocated to foreign intelligence and CI in the US Air Force graphically illustrates the resource distinction between these two disciplines. As of 30 September 2005, there were 14, 286 active duty personnel holding intelligence Air Force specialty codes (AFSCs), and only 1,283 holding the special investigations AFSC.⁹⁶ An

⁹³ The Commission on the Intelligence Capabilities of the US, *Report to the President*, 486, 487, 495.

⁹⁴ Stephen Daggett, *The US Intelligence Budget: A Basic Overview*, (Washington, DC: Congressional Research Service, 4 October 2004), 3.

⁹⁵ The National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, 86.

⁹⁶ “USAF Almanac 2006,” *Air Force Magazine* 89, no. 5 (May 2006): 56.

additional 402 Air Force civilian employees serve as full-time AFOSI special agents.⁹⁷ The fact that the majority of AFOSI's investigative activities pertain to felony crimes such as murder, robbery, rape and assault further exacerbates the resource gap between the intelligence and CI function in the AF.⁹⁸

DOD CI Structural Weaknesses

The current DOD CI structure places an inefficient barrier between military CI activities and the war-fighting role of the COCOMs. Since the operational CI elements within DOD fall under the command and control of the Services, they have a natural tendency to focus on the priorities of their particular Service and generally treat COCOM requirements as secondary priorities. The Service CI agencies primarily operate from major DOD installations and focus their efforts on supporting these installations. This means that in addition to not prioritizing COCOM requirements, DOD CI generally provides little direct support to civilian transportation infrastructure utilized by DOD and other critical infrastructure targets located outside main operating bases.

The WMD Commission noted that the current Service focused CI efforts within DOD fail to provide effective CI protection to many DOD components including COCOMs, Defense Agencies, and the Office of the Secretary of Defense (OSD). The WMD Commission's proposed solution to this problem was to assign full spectrum CI responsibilities to CIFA, including responsibilities to conduct CI collections, investigations, and operations.⁹⁹ Although this proposal might improve direct CI support to OSD, it would do little to improve CI support to

⁹⁷ US Air Force, "Fact Sheet: Air Force Office of Special Investigations," undated, <http://www.osi.andrews.af.mil/library/factsheets/factsheet.asp?id=4848>

⁹⁸ Ibid

⁹⁹ The Commission on the Intelligence Capabilities of the US, *Report to the President*, 494.

the COCOMs. Under the current structure, the Military CI agencies fall under their Service chain of command and are therefore directly responsive to Service priorities. At the same time, the Service CI agencies are at least indirectly responsive to COCOM requirements based on their interaction with the COCOM Service Component Commands. A larger, more powerful CIFA, reporting to the Undersecretary of Defense for Intelligence (USD-I), would have no direct link with either the Services or the COCOMs. There is no reason to believe an expanded CIFA would be any more responsive to COCOM requirements than the current Service CI agencies.

Current Laws and Directives that Impact DOD CI and Investigative Activities

There is no consensus concerning the role the US military should play in Homeland security, to include the appropriate role DOD should play in detecting and neutralizing infiltration threats. This debate becomes especially complex when it comes to discussing the use of DOD intelligence, CI and criminal investigative resources within US society. One of the most frequently cited restrictions on the use of military resources in the United States is the Posse Comitatus Act of 1878.

Although most Americans have likely heard of the Posse Comitatus Act it is doubtful that many, including those in the military, fully understand it. Various authors have offered different interpretations of what the act actually forbids and have articulated differing views on the act's purpose. One of the most common interpretations is that the Posse Comitatus Act forbids any element of the military from engaging in law enforcement functions including arrests, searches, seizure of evidence, surveillance and other "police-type" activities within the United States.¹⁰⁰

¹⁰⁰ For examples of this interpretation see: George C. Kiser, "Military Policing of the United States," *Humanist* 57, no. 3 (May/June 1997): 32-33, Stew Magnuson, "A Cautious Approach to Homeland Security: Pentagon Wary of Posse Comitatus Prohibitions," *Defense News*, 17 November 2003, 28, and Mark Thompson and John F. Dickerson, "Soldier on the Beat," *Time* 158, no. 24 (3 December 2001): 60.

Authors holding this interpretation have stated the act was initially passed “to guard against military dictatorship.”¹⁰¹

Other authors have stressed that in practice the Posse Comitatus Act does not impede the military from participating in law enforcement activities, and contend the act was actually passed to prevent civilian law enforcement officials from calling out, deputizing and controlling the military.¹⁰² Authors holding these views have claimed DOD has used an “extremely broad” interpretation of the act “to ward off undesired and potentially resource-depleting missions.”¹⁰³ A careful examination of the mission responsibilities and authorities granted to military CI and criminal investigative personnel clearly demonstrates that the common perception that the Posse Comitatus Act prevents DOD from performing law enforcement functions is simply incorrect. Special Agents of the Military Criminal Investigative Organizations (MCIOs) are recognized as federal law enforcement officers, and have authority to conduct investigations both on and off military installations.¹⁰⁴ All MCIO Agents are authorized to obtain and serve federal search warrants, and civilian agents of the MCIOs possess arrest authority for violations of US Federal Law.¹⁰⁵

The Intelligence Oversight provisions identified in Executive Order 12333, *United States Intelligence Activities*, serve as another frequently cited restriction on the use of US military resources in the United States. The Intelligence Oversight provisions contained in Executive Order 12333 apply to the entire US Intelligence Community, not just those intelligence and CI

¹⁰¹ Magnuson, “A Cautious Approach to Homeland Security”.

¹⁰² For examples of this interpretation see: Gary Felicetti and John Luce, “The Posse Comitatus Act: Liberation from the Lawyers,” *Parameters* 34, no. 3 (Autumn 2004): 94-107 and Sydney J. Freeburg, Jr, “Posse Comitatus: Tiny Law, Big Impact,” *National Journal* 37, no. 46 (12 November 2005): 3557-3558.

¹⁰³ Gary Felicetti and John Luce, “The Posse Comitatus Act.”

¹⁰⁴ United States Code of Federal Regulations, Title 28, Sections 60.2 and 60.3.

¹⁰⁵ Code of Federal Regulations, Title 28, Sections 60.2 and 60.3 and United States Code, Title 10, Sections 4027, 7480, and 9027.

agencies within the DOD.¹⁰⁶ Some erroneously believe this order restricts military intelligence units from collecting information on US citizens.¹⁰⁷

DOD collection and retention of information on US Persons is primarily governed by two DOD publications. DOD 5240.1R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*, applies to DOD intelligence and CI activities, while DOD Directive (DODD) 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated With the Department of Defense*, applies to security, criminal investigative and law enforcement activities. DOD 5240.1R implements the Intelligence Oversight provisions codified by Executive Order 12333, and generally restricts DOD CI agencies from collecting information on US Persons unless they “are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.”¹⁰⁸ DODD 5200.27 states DOD criminal investigators may acquire information “about activities threatening defense military and civilian personnel and defense activities and installations, including vessels, aircraft, communications equipment, and supplies.”¹⁰⁹ The fact that some DOD agencies including NCIS and AFOSI hold both CI and criminal investigative responsibilities means the determination whether their agents should follow the guidance in DODD 5200.27, or the more restrictive requirements of DOD 5240.1R is based on whether these agents are engaged in CI activities or criminal investigative activities. This can lead to confusion since most NCIS and AFOSI agents routinely operate in both

¹⁰⁶ Executive Order 12333, *United States Intelligence Activities*, 4 December 1981.

¹⁰⁷ For example see: William M. Arkin, “Domestic Military Intelligence is Back,” *washingtonpost.com*, 29 November 2005, http://blog.washingtonpost.com/earlywarning/2005/11/domestic_military_intelligence.html (accessed 16 September 2006).

¹⁰⁸ DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*, December 1982.

¹⁰⁹ DOD Directive 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated With the Department of Defense*, 7 January, 1980.

disciplines, and it is not uncommon to see overlap between the two missions. Regardless, the exemptions identified in these directives provide Military CI agencies and the MCIOs ample authority to collect and retain threat information within the United States.

Issues of Trust and Credibility

Although neither the Posse Comitatus Act nor the Intelligence Oversight restrictions of Executive Order 12333 completely prohibit the military from conducting law enforcement functions or collecting domestic intelligence, these activities remain controversial. In an article entitled “Military Policing of the United States,” George C. Kiser states that military involvement in domestic law enforcement activities “violates basic principles of democracy and American tradition,” and is “a natural enemy of human rights” and “a common characteristic of the earth’s most repressive regimes.”¹¹⁰ Civilian and military defense personnel have also expressed concern about military involvement in law enforcement and domestic intelligence activities. Former Secretary of Defense Caspar Weinberger has remarked that military policing “is extremely repugnant to a democratic society” and goes “way beyond what the military’s role should be.”¹¹¹ US Army Lieutenant Colonel Grant Doty published an editorial in the *Washington Post* in December 2005 that questioned the implications of even a small numbers of military personnel being used to gather intelligence in the United States.¹¹² At least some portion of the concerns surrounding military involvement in domestic activities can be attributed to actions previously taken by military investigators and CI personnel.

Although legal constraints do not pose a wholesale restriction on military involvement in domestic intelligence and law enforcement activities, any effort to expand these activities will

¹¹⁰ Kiser, “Military Policing of the United States,”.

¹¹¹ Ibid

¹¹² Grant Doty, “I’m a Soldier, Not a Spy,” *Washington Post*, 30 December 2005, A27.

face public scrutiny. The public will base their opinion of the appropriateness of military involvement in domestic affairs on the credibility and professionalism of the personnel conducting the activity. Unfortunately, military investigators and CI personnel have taken actions in the past that have damaged their credibility and professionalism. These self-inflicted wounds are one of the key reasons some people are reluctant to see the military play an expanded role in the domestic environment.

Congressional investigations conducted in the 1970s revealed DOD agents had monitored and infiltrated anti-war groups in the United States during the Vietnam War, and gathered information on the political activities and beliefs of private citizens. These activities were fully detailed in a report issued by the Senate Select Committee to Study Government Operations With Respect to Intelligence Activities in April 1976. This Committee found that DOD agents had utilized covert physical and electronic surveillance, informants, and undercover agents to collect information in the United States.¹¹³ These findings led to the issuance of Executive Order 12333 and the previously discussed DOD directives governing the collection and retention of information on US persons.

The abuses of the Vietnam era seem to have been repeated in the aftermath of 9/11 and Operation IRAQI FREEDOM. In December 2005, NBC News reported DOD had used the Threat and Local Observation Notice or TALON program to gather information on peace and anti-war groups who were exercising their constitutional rights to protest government actions. NBC claimed they had obtained access to a secret CIFA generated database, and their review of

¹¹³ For detailed information on domestic collection activities conducted by the US Military during the Vietnam era see: Senate, Select Committee to Study Governmental Operations With Respect to Intelligence Activities, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, 94th Cong., 2nd Sess., 1976 also available on-line at <http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIk.htm>

this database revealed nearly four-dozen entries on anti-war meetings and protests.¹¹⁴ DOD's response to the disclosure that the TALON program had been used to gather data on anti-war protestors was developed over a period of several months. According to NBC, DOD officials initially refused requests for interviews, and a DOD spokesman provided a standard response that, "all domestic intelligence information is properly collected and involves protection of Defense Department installations, interests and personnel".¹¹⁵ Even after discovering irregularities in the TALON Program, David Burtt, the Director of CIFA, refused to disclose the total number of TALON reports his agency had archived stating the number was classified.¹¹⁶

On 13 January 2006, Deputy Secretary of Defense Gordon England directed that all DOD intelligence and CI personnel receive refresher training on the rules governing the collection, retention, and dissemination of information related to US persons. He also ordered CIFA to undertake a review of the TALON database to identify any reports that should not be retained.¹¹⁷ This review eventually disclosed that CIFA had incorrectly maintained 186 protest related reports in the TALON database.¹¹⁸ On 30 March 2006, Secretary England directed that the system "be used to only to report information regarding possible international terrorist activity and that all TALON reports should be retained in accordance with DOD 5240.1R."¹¹⁹

Given the controversy surrounding the Department of Justice's effort to implement the Terrorist Information and Prevention or (TIPS) program in 2002, (a program designed to

¹¹⁴ Lisa Myers et al., "Is the Pentagon Spying on Americans"?, *MSNBC.com*, 14 December 2005, <http://msnbc.msn.com/id/10454316/> (accessed 9 September 2006).

¹¹⁵ Lisa Myers et al., "Is the Pentagon Spying on Americans".

¹¹⁶ Walter Pincus, "Unverified Reports of Terror Threats Linger; Pentagon Faults 1% of Database Entries", *Washington Post*, 31 January 2006, Final Edition.

¹¹⁷ Gordon England, Deputy Secretary of Defense, to the Secretaries of the Military Departments et al., memorandum, 13 January 2006.

¹¹⁸ Robert W. Rogalski, Deputy Under Secretary of Defense, Acting (Counterintelligence and Security), to Senator Patrick J. Leahy, Ranking Member, Committee on the Judiciary, United States Senate, letter, 8 March 2006.

¹¹⁹ Gordon England, Deputy Secretary of Defense, to the Secretaries of the Military Departments et al., memorandum, 30 March 2006.

encourage private citizens to report suspicious incidents) and the historical lessons of the Vietnam era, DOD leaders should have anticipated the TALON program would be highly scrutinized by Congress and the public.¹²⁰ For this reason, DOD leaders made a critical error when they failed to build adequate safeguards within the program to prevent abuses and detect and remove unauthorized reports.¹²¹

¹²⁰ For information on the debate surrounding the DOJ TIPS Program see: Associated Press, “Safety or Stasi,” *CBS News*, 17 July 2002, <http://www.cbsnews.com/stories/2002/07/17/national/main515404.shtml> (accessed 8 October 2006). And American Civil Liberties Union, “Republican Majority Leader Arney Rejects White House Plans for Operation TIPS, National ID,” 18 July 2002, <http://www.aclu.org/natsec/spying/12498prs20020718.html> (accessed 8 October 2006).

¹²¹ For additional details on the DOD TALON Program see: LtCol Michael T. Imbus, “Department of Defense Threat and Local Observation Notice (TALON) program: Valuable Anti-terrorism Tool or Threat to Civil Liberties?” (Terrorism Elective Paper, Air War College, Maxwell AFB, AL, 12 October 2006).

Chapter 7

Recommendations and Conclusions

The United States has invested in technologically advanced platforms like ballistic missile defense and the F-22 to help counter certain threats to the Homeland and the anti-access strategies of potential adversaries. Since 1985, the United States has spent nearly \$100 billion in an effort to develop and field a capable missile defense system, and the F-22 has an estimated “flyaway” cost of \$133 million per aircraft.¹²² The attention and financial resources focused towards these programs properly address significant threats to the US Homeland and US freedom of action abroad. Unfortunately, none of these programs address the infiltration threat to the Homeland, and the impact this threat could conceivably have on the US military’s ability to quickly deploy forces in a crisis situation. For the fraction of the cost the United States has spent on ballistic missile defense and the development of the F-22, DOD could improve its CI capabilities and more effectively counter infiltration threats to the Homeland.

The US Government has also devoted significant energy and financial resources to counter terrorism in the post 9/11 environment. Although these anti-terrorism measures are a step in the right direction, the United States has not yet taken actions to address the full spectrum of infiltration threats to the Homeland. CI is one of the primary tools that can counter infiltration

¹²² Missile Defense Agency, “Historical Funding for MDA FY85-07,” <http://www.mda.mil/mdalink/pdf/histfunds.pdf> (accessed 2 December 2006) and James W. Crawley, “Cost of F-22 Raptor is Sky High, Critics Allege,” *Richmond Times*, 2 March 2006 http://www.timesdispatch.com/servlet/Satellite?pagename=RTD/MGArticle/RTD_BasicArticle&c=MGArticle&cid=1137834438256&path=!health!healthology.

threats, but unfortunately the US Intelligence Community and DOD have generally treated CI as an adjunct requirement and failed to devote adequate attention and resources to this essential discipline.¹²³ DOD CI currently suffers from a lack of resources, and is hampered by structural weaknesses that impede its ability to properly counter the full range of infiltration threats to the Homeland.

Moving Beyond Terrorism to a Focus on Full-Spectrum Infiltration Threats

The United States took several significant actions in the aftermath of the 9/11 attacks to improve its ability to defend the Homeland from terrorist attack. These actions have included the establishment of the Department of Homeland Security and USNORTHCOM. Although the focus on countering terrorist threats in the post-9/11 environment is understandable, focusing too much attention on the threat posed by al Qaeda and other transnational terrorist organization has caused the US government to focus less attention on the infiltration threats posed by the intelligence and SOF elements of foreign nations. As highlighted by the WMD Commission, “counterintelligence has generally lost stature since September 11, eclipsed by more immediate counterterrorism needs.”¹²⁴

The first step in improving the United State’s ability to counter the infiltration threat to the Homeland is to develop and adopt an analytical framework capable of examining the full-spectrum of infiltration threats including terrorism, sabotage, assassination and espionage. Simply put, it is impossible to counter a threat you do not understand. This framework must be able to define not only the threat posed by non-state actors such as transnational terrorist organizations, but also describe threats posed by potential state adversaries. The analytical

¹²³ The Commission on the Intelligence Capabilities of the US, *Report to the President*, 486-490.

¹²⁴ *Ibid*, 487.

framework presented in Chapter Three of this paper provides a starting point for expanding US government analytical efforts from terrorism to all categories of infiltration threats.

As the lead US Government agency for both CI and counterterrorism, the FBI should continue to play a major role in countering infiltration threats. As discussed in Chapter Six, the FBI has taken positive steps to enhance the interaction between FBI personnel conducting CI and counterterrorism investigations. The FBI should continue this trend by expanding the charter of the current JTTFs to include the traditional CI missions of countering foreign directed espionage, sabotage, and assassination operations. These organizations should transition from JTTFs to Joint National Security Task Forces (JNSTFs), and hold primary responsibility for investigating the full spectrum of infiltration threats to the Homeland including transnational terrorism, international criminal activity, state-sponsored terrorism, sabotage operations, assassination, and espionage and other foreign intelligence activities. These task forces would continue to be led by the FBI and include representatives from DHS, DOD, and other federal, state and local law enforcement and security personnel. DOD CI agencies and the MCIOs should continue to maintain and expand their presence within these FBI-led task forces.

Meeting the CI Challenges of 21st Century

The 2005 National Defense Strategy recognizes the United States is a “nation at war” and gives top priority to “dissuading, deterring, and defeating those who seek to harm the United States directly, especially extremist enemies with weapons of mass destruction.” This document stresses the role of CI in supporting DOD strategy, planning and decision making, and recognizes that the United States itself serves as DOD’s “premier base of operation.”¹²⁵

¹²⁵ Department of Defense, *The National Defense Strategy of the United States of America*, (Washington DC: Office of the Secretary of Defense, March 2005), 1,7,15-16.

Although the 9/11 attacks demonstrated the ability of operatives to strike the US Homeland from within, DOD remains externally focused and exerts little effort to counter foreign directed threats emanating from inside US borders. Despite the fact the threat environment has drastically changed over the past 20 years, the resource balance between foreign intelligence and CI activities across DOD remains essentially unchanged from the Cold War era. This balance needs to be reevaluated. In an era where terrorism and other asymmetric threats serve as the primary threat to the Homeland, it no longer makes sense for the Air Force and the other Services to devote the vast majority of their intelligence resources to foreign intelligence activities, while devoting only minimal resources to CI activities.

In addition to rebalancing the resources allocated to DOD foreign intelligence and CI activities, DOD CI and MCIO authorities be strengthened in order to allow DOD agents to play an appropriate role in interagency efforts to counter infiltration threats to the Homeland. Congressional action to modify Title 10 of the United States Code and specifically grant arrest authority to civilian special agents assigned to the MCIOs was a positive step, but DOD should also seek civilian arrest authority for military special agents. Gaining this authority would remove a significant distinction between civilian and military agents who possess identical experience and training, and ease personnel management and assignment actions for those MCIOs with a large percentage of military agents.¹²⁶

Any effort to increase DOD's involvement in domestic intelligence gathering and law enforcement activities will likely face resistance from both civilian and military commentators. One argument against increased DOD involvement in these activities is centered on the belief that military personnel are neither familiar with US Constitutional principles and protections nor

¹²⁶ For example, AFOSI has 1,154 active duty military special agents and 379 reserve military agents compare to 402 civilians. Information from: US Air Force, "Fact Sheet: Air Force Office of Special Investigations."

trained to conduct law enforcement activities. The other argument is based on the belief that increased military involvement in domestic activities will harm military readiness.¹²⁷ These arguments consider the military as a whole, and do not take into account the unique training and experience of particular military units like DOD CI agencies or the MCIOs. DOD needs to move the argument regarding military participation in domestic activities beyond treating the entire US military as a single entity, and instead focus on the precise skill sets and missions of specific units.

The average infantry soldier may not receive training on constitutional protections or law enforcement tactics, but special agents assigned to the MCIOs receive considerable training in these areas. At the current time, AFOSI and NCIS agents attend basic investigative training at the Federal Law Enforcement Training Center (FLETC) in Glynco, GA, and their initial training is identical to that received by many of their federal law enforcement counterparts.¹²⁸ The FLETC training program is managed by DHS, and FLETC serves as the training center for numerous federal law enforcement agencies including the US Secret Service, Immigration and Customs Enforcement, and the US Marshals Service.¹²⁹ In addition, there is little difference between the wartime and peacetime missions of the DOD CI agencies and the MCIOs. Criminal activity, foreign directed espionage and other intelligence activities, and terrorism occur throughout the spectrum of conflict. Conducting CI collections and operations, and performing CI and criminal investigations is both the wartime and peacetime mission of these agencies.

¹²⁷ Information on these arguments can be found in: Kiser, "Military Policing of the United States", Juliette N. Kayyem and Steven E. Roberts, "War on Terrorism Will Compel Revisions to Posse Comitatus," *National Defense* 87, no. 589 (December 2002): 41, and Thompson and Dickerson, "Soldier on the Beat."

¹²⁸ Naval Criminal Investigative Service, "Frequently Asked Questions," <http://www.ncis.navy.mil/about/faqs.asp> (accessed 30 January 2007), and US Air Force, "Fact Sheet: Air Force Office of Special Investigations."

¹²⁹ Federal Law Enforcement Training Center, "About FLETC," <http://www.fletc.gov/about-fletc/about-fletc> (accessed 31 January 2007).

Public acceptance of increased DOD involvement in law enforcement and domestic intelligence activities will require DOD to maintain the trust of the American people. Coupled with the excesses of the Vietnam era, the recent disclosures the TALON program was used to collect information on peace activities and anti-war movements was a damaging self-inflicted wound to the credibility and professionalism of DOD CI and investigative agencies. The fact DOD failed to respond to these mistakes before they were highlighted by the media was inexcusable and demonstrates that although training and oversight programs were in place, they were insufficient to prevent and respond to program abuses. DOD leaders must ensure training and oversight programs are bolstered to prevent any future abuses. If abuses occur, they must be detected and corrective action must be taken immediately in full view of the public in order to maintain trust and credibility.

Improving the Connection Between DOD CI and the War Fighting Role of the COCOMs

In addition to resource and authority shortfalls, the DOD CI community suffers from structural and organizational weaknesses that separate DOD CI capabilities and activities from the war-fighting mission of the COCOMs. The DOD CI community must take action to address this disconnect while still allowing the Service Secretaries to maintain the CI and investigative authorities and resources needed to fulfill their Title 10 responsibilities. The WMD Commission recognized this disconnect and proposed significant changes to the overall structure and authorities of the DOD CI agencies.¹³⁰ The far-reaching changes proposed by the WMD Commission are neither necessary nor warranted. DOD can take the necessary actions to better

¹³⁰ The Commission on the Intelligence Capabilities of the US, *Report to the President*, 493-495.

balance CI authorities between the COCOMs and the Services by following existing CI directives and doctrine and capitalizing on the existing wartime authorities of the COCOMs.

The actions of al Qaeda and its associated networks have shown that the Global War on Terrorism (GWOT) has no geographic boundaries. Although the bulk of military action in the GWOT has occurred in the US Central Command (USCENTCOM) area of responsibility, this does not mean the forces under the other COCOMs are not also engaged in this war. The GWOT is a worldwide effort and every regional COCOM has an active role to play in the ultimate success of this effort. As the DOD element with primary responsibility for Homeland Defense missions, USNORTHCOM's role in the GWOT is to protect the United States from terrorist and other externally directed aggression. USNORTHCOM performs this mission in coordination with DHS, the FBI, and other civilian agencies.¹³¹

As this paper has shown, terrorist organizations are not the only elements that pose infiltration threats to the Homeland. Based on this reality, the United States should not only be conducting a war against international terrorism, but should also be working to identify foreign adversaries seeking to infiltrate the United States to conduct espionage, assassinations or sabotage operations. Foreign adversaries are conducting espionage against the United States now, and are building the networks and plans that could allow them to conduct sabotage strikes or assassinations within the US Homeland in the event of hostilities. DOD CI must have the resources and structure to detect and counter these threats as they develop. Waiting until an enemy strikes the Homeland is simply unacceptable.

DOD activities to defend against the full spectrum of infiltration threats are an important part of the overall Homeland Defense effort, and should be reflected in appropriate Operation

¹³¹ Department of Defense, *Homeland Security Joint Operating Concept* (Peterson AFB, CO: USNORTHCOM, February 2004), 1-2.

NOBLE EAGLE Operations Orders (OPORDS). In part, these OPORDS should assign OPCON of designated Military Service CI forces to the Commander of USNORTHCOM. As a starting point, USNORTHCOM should have OPCON of all DOD agents currently detailed to the FBI led JTTFs, and have OPCON of a multi-service CI element tasked with providing direct support to USNORTHCOM Headquarters. USNORTHCOM would retain the option to request additional forces if needed to support emerging operations. The Services should continue to maintain administrative control (ADCON) of these agents in order to allow them to maintain their Title 10 CI investigative and operational authorities. The Commander, USNORTHCOM should exercise OPCON of these CI forces through his assigned CISO. Each Military Service CI agency should assign a liaison officer to the USNORTHCOM CISO to aid in the communication of taskings, and represent Service interests. In addition, DOD CI policies should be modified to eliminate the current separation between those CI activities COCOMs can and cannot control in a wartime environment. Clarification of these policies would allow COCOMs to direct all CI activities and law enforcement functions conducted by DOD special agents under their OPCON.

Although this proposal may face resistance from the Service CI agencies, it provides a mechanism to balance Service and COCOM CI needs. This proposal would allow the Services to maintain needed CI capabilities, while better linking DOD CI to the Homeland Defense mission of USNORTHCOM. The Services would continue to maintain full control over CI elements supporting Service activities and functions at main operating bases. USNORTHCOM would gain control over DOD CI activities directly supporting Homeland Defense activities such as CI support to critical infrastructure protection. This proposal would also build the confidence of the American public by placing DOD agents operating outside geographical areas housing main DOD installations under what would essentially be the tactical control (TACON) of FBI

supervisory personnel within the JTTFs or JNSTFs. This would provide solid civilian oversight of military domestic law enforcement and intelligence gathering activities.

The National Strategy for Combating Terrorism recognizes that the United States must use all elements of national power in the fight against terrorism. Among the key capabilities used to fight terrorism, military action, law enforcement activities, and intelligence collection and analysis play important roles.¹³² DOD CI and criminal investigative special agents operate in both the law enforcement and intelligence realms, and are under the military services. Given their training and mission responsibilities, these agents can serve as effective coordinators between the military and civilian agencies involved in law enforcement and intelligence activities. To meet its Homeland Defense responsibilities, USNORTHCOM must have the ability to take full advantage of DOD special agents' unique skills and access to civilian counterparts. Providing USNORTHCOM OPCON over the activities of some DOD agents would provide the command this vital capability.

Conclusion

Although the United States has dedicated considerable effort and resources to countering terrorist threats to the Homeland, these measures have not addressed the full range of infiltration threats faced by the Nation. History has shown that the infiltration threat to the United States consists not only of terrorism, but also espionage, assassination and sabotage activities conducted by agents and operatives from hostile and potentially hostile regimes. Germany carried out sabotage and intelligence operations within the United States during both World Wars and we must anticipate that future adversaries will also seek to conduct similar activities. These future

¹³² *National Strategy for Combating Terrorism* (Washington DC: The White House, September 2006), 1.

adversaries may have previously developed contingency plans and may already have operatives in the United States ready to conduct attacks.

To understand the full scope of the infiltration threat to the United States, the US intelligence and security communities must move beyond current analytical methodologies and threat advisory systems focused solely on terrorism, and develop an analytical framework that examines the full spectrum of infiltration threats. This paper provides a starting point for the development of an analytical framework of this type, and uses this framework to demonstrate the potential infiltration threat posed by China.

CI is one of the essential tools in the effort to counter infiltration threats. Despite this, the WMD Commission found resource and structural weaknesses that negatively impact the US CI Community's ability to meet the challenge posed by foreign directed espionage and other threats. DOD CI is not immune from these problems. Despite the changes in the threat environment in the post Cold War and 9/11 world, DOD continues to focus the bulk of its intelligence efforts on foreign intelligence activities and devotes minimal resources to CI activities. The balance between foreign intelligence and CI resources must be reevaluated given the current threat environment. In addition to these resource shortfalls, DOD CI also suffers from structural weaknesses that tend to separate CI activities from the war-fighting mission of the COCOMs. Although the WMD Commission recommended major changes in the organization and authority of DOD CI elements to address these weaknesses, this paper recommends a solution that relies on existing DOD CI doctrine and directives. This solution recognizes the COCOM authority over Service CI activities during wartime operations, and proposes that certain DOD CI agents be placed under the OPCON of USNORTHCOM for the duration of Operation NOBLE EAGLE.

This solution would balance Service and COCOM CI needs, while granting USNORTHCOM direct control of CI activities directly related to ongoing Homeland Defense activities.

By better analyzing and understanding infiltration threats, clarifying DOD's role in countering these threats, and enhancing the connection between DOD CI activities and the Homeland Defense mission of USNORTHCOM, DOD can improve its ability to counter the full range of infiltration threats and more effectively protect the Homeland.

Bibliography

- Air China. "English Language Homepage." <http://www.airchina.com.cn/index.jsp> (Accessed 1 November 2006).
- American Civil Liberties Union, "Republican Majority Leader Arney Rejects White House Plans for Operation TIPS, National ID." 18 July 2002, <http://www.aclu.org/natsec/spying/12498prs20020718.html> (accessed 8 October 2006).
- Arkin, William M. "Domestic Military Intelligence is Back." *Washingtonpost.com*, 29 November 2005, http://blog.washingtonpost.com/earlywarning/2005/11/domestic_military_intelligence.html (accessed 16 September 2006).
- Associated Press. "Safety or Stasi." *CBS News*, 17 July 2002, <http://www.cbsnews.com/stories/2002/07/17/national/main515404.shtml> (accessed 8 October 2006).
- Bielling, Patti. "Anchorage is Named DOD's Newest Strategic Seaport." *Military Surface Deployment and Distribution Command Public Affairs Release*, 17 August 2004.
- Berman, Ilan. *Tehran Rising*. Lanham, MD: Rowman & Littlefield Publishers, Inc., 2005.
- Bermudez, Joseph S. Jr. *North Korean Special Forces*, 2nd ed. Annapolis, MD: Naval Institute Press, 1998.
- Beeston, Richard and Daniel McGrory. "Poison Plotters Claim Their Second Victim." *Times Online*, 2 December 2006 <http://www.timesonline.co.uk/article/0,,2-2482990,00.html>.
- Bijian, Zheng. "China's Peaceful Rise and Asia's New Role." Beijing: Xuexi Shibao, 2 May 2005.
- Brookes, Peter. "Legion of Amateurs: How China Spies." *The Heritage Foundation*, 31 May 2005 <http://www.heritage.org/Press/Commentary/ed053105c.cfm>.
- Brookes, Peter. "The Spies Among Us." *The Heritage Foundation*, 1 June 2006, <http://www.heritage.org/Press/Commentary/ed060106c.cfm>.
- Brookes, Peter. "Spooks, Lies and Videotape." *The Heritage Foundation*, 6 July 2004, <http://www.heritage.org/Press/Commentary/ed070604a.cfm>.

- Cameron, Gavin, Jason Pate and Kathleen Vogel. "Planting Fear, How Real is the Threat of Agricultural Terrorism." *Bulletin of the Atomic Scientists* 57, no. 05 (2001) http://www.thebulletin.org/article.php?art_ofn=so01cameron.
- Carter, Sara A. "Of Special Interest: U.S. Agencies Missing Links Between Illegal Immigration And Terrorism." *San Bernardino Sun*, 29 December 2006, http://www.sbsun.com/news/ci_4917538.
- The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States*. Washington DC: The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 31 March 2005, also available at <http://www.wmd.gov/report/index.html>.
- Conrad, Scott W. *Moving the Force: Desert Storm and Beyond*. Washington, DC: Institute for National Strategic Studies, 1994.
- Cordesman, Anthony H. *Iran's Developing Military Capabilities*. Washington, DC: Center for Strategic and International Studies, 2005.
- Crawley, James W. "Cost of F-22 Raptor is Sky High, Critics Allege." *Richmond Times*, 2 March 2006 http://www.timesdispatch.com/servlet/Satellite?pagename=RTD/MGArticle/RTD_BasicArticle&c=MGArticle&cid=1137834438256&path=!health!healthology.
- Daggett, Stephen. *The US Intelligence Budget: A Basic Overview*. Washington, DC: Congressional Research Service, 4 October 2004.
- Department of Defense. *Homeland Security Joint Operating Concept*. Peterson AFB, CO: USNORTHCOM, February 2004.
- Department of Defense. *The National Defense Strategy of the United States of America*. Washington DC: Office of the Secretary of Defense, March 2005.
- Department of Defense. *Quadrennial Defense Review Report*. Washington DC: Department of Defense, 6 February 2006.
- Department of State. *Country Reports on Terrorism 2005*. Washington DC: Department of State Office of the Coordinator for Counterterrorism, April 2006.
- Department of State. *Foreign Consular Offices in the United States Spring/Summer 2006*. Washington DC: Superintendent of Documents, US Government Printing Office, 4 August 2006.
- Director of Federal Bureau of Investigation and Director of Central Intelligence Agency. "Report to Congress on Chinese Espionage Activities Against the United States."

- Washington DC, 1999.
- DOD 5240.1-R. *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*, December 1982.
- DOD Directive 5105.67. *Department of Defense Counterintelligence Field Activity*, 19 February 2002.
- DOD Directive 5200.27. *Acquisition of Information Concerning Persons and Organizations Not Affiliated With the Department of Defense*, 7 January, 1980.
- DOD Directive 5240.2. *DOD Counterintelligence*, 22 May 1997.
- DOD Instruction 5240.10. *Counterintelligence Support to the Combatant Commands and the Defense Agencies*, 14 May 2004.
- Doty, Grant. "I'm a Soldier, Not a Spy." *Washington Post*, 30 December 2005, A27.
- Eftimiades, Nicholas. *Chinese Intelligence Operations*. Annapolis, MD: Naval Institute Press, 1994.
- England, Gordon, Deputy Secretary of Defense. To the Secretaries of the Military Departments et al. Memorandum, 13 January 2006.
- England, Gordon, Deputy Secretary of Defense. To the Secretaries of the Military Departments et al. Memorandum, 30 March 2006.
- Executive Order 12333. United States Intelligence Activities. 4 December 1981.
- Federal Law Enforcement Training Center. "About FLETC."
<http://www.fleetc.gov/about-fleetc/about-fleetc> (accessed 31 January 2007).
- Federal Maritime Commission. "China Ocean Shipping Company."
<http://www.fmc.gov/reading/ChinaOceanShippingCompany.asp> (accessed 1 November 2006).
- Feickert, Andrew. *US Special Operations Forces (SOF): Background and Issues for Congress*. Washington, DC: Congressional Research Service, 28 September 2004.
- Felicetti, Gary and John Luce. "The Posse Comitatus Act: Liberation from the Lawyers."
Parameters 34, no. 3 (Autumn 2004): 94-107.

- Flanagan, Stephen J. and Michael E. Marti. "The PLA in a Changing China: An Overview." in *The People's Liberation Army and China in Transition*. Edited by. Stephen J. Flanagan And Michael E. Marti. Washington DC: National Defense University Press, 2005.
- Freeburg, Sydney J. Jr. "Posse Comitatus: Tiny Law, Big Impact." *National Journal* 37, no. 46 (12 November 2005): 3557-3558.
- General Accounting Office. *Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployments Through Domestic Seaports*. Washington, DC: General Accounting Office, October 2002.
- Gilbert, Craig. "Hart Senate Office Building Reopens." *Milwaukee Journal Sentinel*, 23 January 2002.
- Godwin, Paul H.B. "PLA Doctrine and Strategy: Mutual Apprehension in Sino-American Military Planning," in *The People's Liberation Army and China in Transition*. Edited by Stephen J. Flanagan and Michael E. Marti. Washington DC: National Defense University Press, 2005.
- Gordon, Michael R. and Bernard E Trainor. "Even as U.S. Invaded, Hussein Saw Iraqi Unrest as Top Threat." *New York Times*, 12 March 2006.
- Henderson, Scott J. "In the Shadow: Chinese Special Forces Build a 21st Century Fighting Force." *Special Warfare* 19, no. 4 (July/August 2006): 30-35.
- Homeland Security Presidential Directive-3, 11 March 2002.
- Imbus, LtCol Michael T. "Department of Defense Threat and Local Observation Notice (TALON) program: Valuable Anti-terrorism Tool or Threat to Civil Liberties?" Terrorism Elective Paper, Air War College, Maxwell AFB, AL, 12 October 2006.
- Institute of International Education. "U.S. Sees Slowing Decline in International Student Enrollment in 2004/2005." <http://opendoors.iienetwork.org/?p=69736> (accessed 19 October 2006).
- "Iraqi Envoy's Son Charged." *Washington Post*, 15 April 2003.
- Jeffrey, Terrence P. "How Saddam Tried to Kill Bush." *Human Events* 58, no. 36 (30 September 2002).
- Jehl, Douglas. "Iraqi Tells FBI He Led Attempt to Kill Bush, US Officials Say." *New York Times*, 20 May 1993.
- Joint Publication 1.02. *DOD Dictionary of Military and Associated Terms*, 8 August 2006, <http://www.dtic.mil/doctrine/jel/doddict/>.
- Kayyem, Juliette N. and Steven E. Roberts. "War on Terrorism Will Compel Revisions to Posse

- Comitatus.” *National Defense* 87, no. 589 (December 2002): 41.
- Kiser, George C. “Military Policing of the United States.” *Humanist* 57, no. 3 (May/June 1997): 32-33.
- Knickerbocker, Brad. “Illegal Immigrants in the US: How Many are There?” *The Christian Science Monitor*, 16 May 2006 <http://www.csmonitor.com/2006/0516/p01s02-ussc.htm>.
- Lang, Colonel Qiao and Colonel Wang Xiangsui. *Unrestricted Warfare; China’s Master Plan to Destroy America*. Panama City, Panama: Pan American Publishing Company, 2002.
- Larson, Eric V. et al. *Assuring Access in Key Strategic Regions*. Santa Monica, CA: Rand Corporation, 2004.
- Linzi, Lu. “Preemptive Strikes Crucial in Limited High Tech Wars.” *Jiefangjun Bao*, February 14, 1996.
- Looney, Robert. “Economic Costs to the United States Stemming from the 9/11 Attacks.” *Center for Contemporary Conflict*, 5 August 2002.
<http://www.ccc.nps.navy.mil/rsepResources/si/aug02/homeland.asp>.
- Lunev, Stanislav. “China’s Intelligence Machine (Overseas Intelligence Activities).” *Insight on the News*, 13, no. 42 (Nov 17, 1997).
- Magnuson, Stew. “A Cautious Approach to Homeland Security: Pentagon Wary of Posse Comitatus Prohibitions.” *Defense News*, 17 November 2003, 28.
- Maier, Timothy W. “China’s Military May Get US Base.” *Insight on the News* 15, no. 18 (17 May 1999).
- Mearsheimer, John J. “China’s Unpeaceful Rise.” *Current History* 105, no. 690 (April 2006), 160-162.
- Menarchik, Douglas. *Powerlift—Getting to Desert Storm*. Westport, CT: Praeger Publishers, 1993.
- Missile Defense Agency. “Historical Funding for MDA FY85-07.”
<http://www.mda.mil/mdalink/pdf/histfunds.pdf> (accessed 2 December 2006).
- Mrozinski, Lawrence G. et al. “Countering China’s Threat to the Western Hemisphere.” *International Journal of Intelligence and Counterintelligence* 15, no. 2 (Summer 2002): 195-210.
- Mueller, Robert S. III. Director, Federal Bureau of Investigation. Statement Before the House Appropriations Subcommittees on Science, Justice and Commerce, and Related Agencies. 14 September 2006, also available online at <http://www.fbi.gov/congress/congress06/mueller091406.htm>.

Myers, Lisa et al. "Is the Pentagon Spying on Americans?" *MSNBC.com*, 14 December 2005, <http://msnbc.msn.com/id/10454316/> (accessed 9 September 2006).

The National Commission on Terrorist Attacks Upon the United States. *9/11 Commission Report*. Washington DC: Government Printing Office, 22 July 2004, 169,229, also available online at <http://www.9-11commission.gov/report/index.htm>.

National Strategy for Combating Terrorism. Washington DC: The White House, September 2006.

Naval Criminal Investigative Service. "Frequently Asked Questions." <http://www.ncis.navy.mil/about/faqs.asp> (accessed 30 January 2007).

Ng, Ka Po. *Interpreting China's Military Power*. New York: Frank Cass, 2005.

O'Donnell, Pierce. *In Time of War*. New York: The New Press, 2005.

"The Overlooked Attack." *Washington Post*, 12 July 2005.

Permanent Mission of the People's Republic of China to the United Nations. <http://www.china-un.org/eng/> (Accessed 1 November 2006).

Pierre, Robert E. "Editor Acted as Iraqi Agent, U.S. Charges." *Washington Post*, 10 July 2003.

Pincus, Walter. "Unverified Reports of Terror Threats Linger; Pentagon Faults 1% of Database Entries." *Washington Post*, 31 January 2006, Final Edition.

Rogalski, Robert W. Deputy Under Secretary of Defense, Acting (Counterintelligence and Security). To Senator Patrick J. Leahy. Ranking Member, Committee on the Judiciary, United States Senate. Letter, 8 March 2006.

Smith, Xavier Gerard. "Special Operations Forces in the People's Liberation Army and the Development of an Integral Unconventional Warfare Mission." Master's Thesis, Naval Postgraduate School, June 2005.

Thompson, Mark and John F. Dickerson. "Soldier on the Beat." *Time* 158, no. 24 (3 December 2001): 60.

Thornburgh, Nathan. "The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)." *Time*, 29 August 2005, <http://www.time.com/time/magazine/article/0,9171,1098961-1,00.html>.

"USAF Almanac 2006." *Air Force Magazine* 89, no. 5 (May 2006): 56.

US Air Force. "Fact Sheet: Air Force Office of Special Investigations." undated, <http://www.osi.andrews.af.mil/library/factsheets/factsheet.asp?id=4848>.

- US Army Criminal Investigations Command. "US Army Criminal Investigations Command Mission." <http://www.cid.army.mil/mission.htm> (accessed 20 January 2007).
- US China Economic and Security Review Commission. *2005 Report to Congress of the U.S. China Economic and Security Review Commission*. 109th Cong., 1st sess, November 2005.
- United States Code of Federal Regulations, Title 28, Sections 60.2 and 60.3.
- United States Code, Title 10, Sections 4027, 7480, and 9027.
- US Customs and Border Protection. *Performance and Accountability Report, Fiscal Year 2006*. Washington, DC: 15 November 2006.
- US House. *Report of the Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China*. 105th Cong., 2d sess., 1999, Report 105-851.
- US Senate. Select Committee to Study Governmental Operations With Respect to Intelligence Activities. *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*. 94th Cong., 2nd Sess., 1976 also available on-line at <http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIk.htm>.
- US Senate. S. Res. 187, 107th Cong., 1st sess., 2001.
- US Transportation Command, "About USTRANSCOM." <http://www.transcom.mil/organization.cfm> (accessed 23 November 2006).
- Waller, J. Michael. "PLA Revises the Art of War." *Insight on the News* 16, no. 8 (28 February 2000): 21.
- Warner, Michael. "The Kaiser Sows Destruction." *Studies in Intelligence* 46, no. 1 (2002) <https://www.cia.gov/csi/studies/vol46no1/index.html>.
- Weiser, Benjamin. "Another Son of Iraqi Ex-Diplomat Indicted." *New York Times*, 6 September 2003.
- Wortzel, Larry M. Ph. D. "Risks and Opportunities of a Rising China." Lecture, Conference on The Asian Century for Business: A Security Challenge, Washington DC, 23 May 2006. <http://www.heritage.org/Research/AsiaandthePacific/h1948.cfm>.