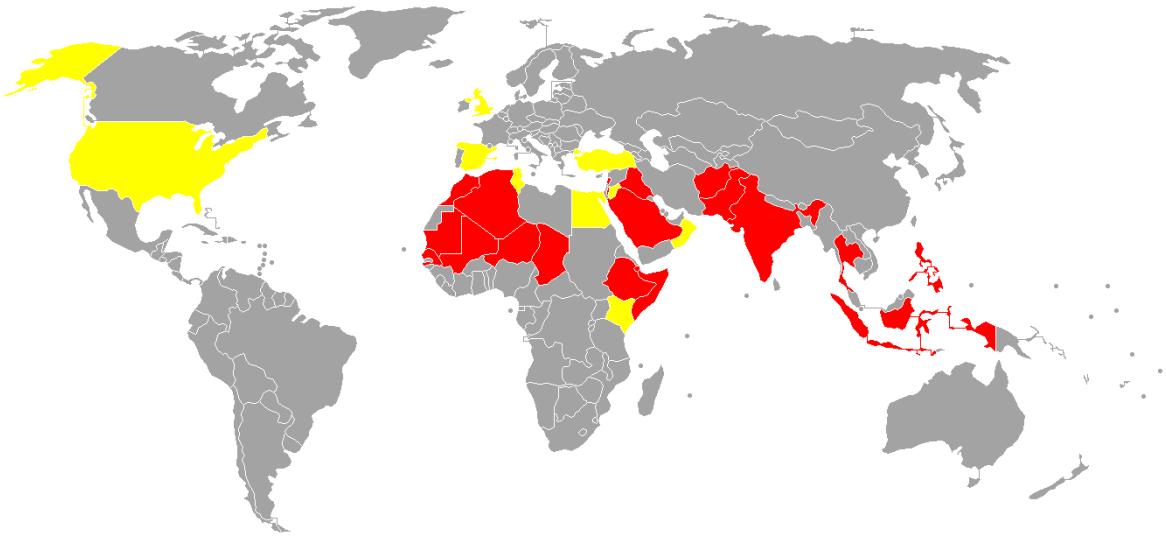
An Index to the Microfilm Edition of

Studies in Global Crisis

The Global War on Terrorism



Primary Source Media

GALE
CENGAGE Learning

The Global War on Terrorism

Primary Source Media

GALE
CENGAGE Learning

Primary Source Media

Studies in Global Crisis:
The Global War on Terrorism

ISBN: 978-1-57803-425-6

Primary Source Media
12 Lunar Drive, Woodbridge, CT 06525
Tel: (800) 444-0799 and (203) 397-2600
Fax: (203) 397-3893

Visit the Primary Source Media website at **www.gale.cengage.com/psm**
Visit Gale online at **www.gale.cengage.com**
Visit our corporate website at **www.cengage.com**

Cover photograph: A map depicting the battlefields in the international war on terror. Red indicates nations in which military efforts are being made to fight terrorism, as defined by the Bush Administration's definition of the war on terror. Countries in yellow have been hit by attacks by to the organizations being targeted in the war on terror, but are not the sites of military efforts. From Wikimedia.

Printed in the United States of America

TABLE OF CONTENTS

SCOPE AND CONTENT NOTE

> *"The war we are fighting today against terrorism is a multifaceted fight. We have to use every tool in our toolkit to wage this war - diplomacy, finance, intelligence, law enforcement, and of course, military power - and we are developing new tools as we go along."* Richard Armitage

In the 1990s, the number and scale of terrorist incidents had risen each year, forcing political terrorism upon the consciousness of the American people. At the same time, policymakers struggled to formulate an effective and coherent strategy to combat terrorist acts, both domestically and abroad.

Early in the morning on September 11, 2001, nineteen hijackers took control of four commercial airliners en route to San Francisco and Los Angeles from Boston, Newark, and Washington, D.C. At 8:46 a.m., American Airlines Flight 11 was crashed into the World Trade Center's North Tower, followed by United Airlines Flight 175 which hit the South Tower at 9:03 a.m. Another group of hijackers flew American Airlines Flight 77 into the Pentagon at 9:37 a.m. A fourth flight, United Airlines Flight 93, whose ultimate target was thought to be either the United States Capitol or White House, crashed near Shanksville, Pennsylvania at 10:03 a.m. Within an hour and a half, international terrorism decimated American hearts and minds.

In the immediate aftermath of the attacks, the Bush administration announced a war on terrorism, a global war. The stated objectives of the war were to protect America, break up terrorist cells in the U.S., and disrupt the activities of the international network of terrorist organizations made up of a number of groups under the umbrella of al-Qaeda.

But, the term and the policies it denotes have been a source of ongoing controversy, as critics have argued that it has been used to justify unilateral preemptive war, human rights abuses and other violations of international law.

> *"To win the war on terror, we must know who our friends are and where our enemies are hiding. We can't continue fighting terrorism using the same foreign policy blueprints that were in place before September 11th."* Evan Bayh

Primary Source Media's new microfilm series documents the U.S. response to the threat posed by international terrorism and the ongoing global conflict to eradicate terrorism. The research behind the studies, reports, and analyses represents an exhaustive review of the facts, causes, and political and military implications of a phenomenon that threatens every region of the world.

The Global War on Terrorism assembles research studies that analyze the goals and strategies of global terrorism. Theses studies, reports, and analyses were conducted by governmental agencies, and private organizations under contract with the Federal government. They represent the most rigorous and authoritative research on the global war on international and domestic terrorism.

The documents in this collection are diverse in scope and emphasis. They dissect specific terrorist events, explore the goals beyond the violence, illuminate the psychology of terrorism, trace the origins and development of terrorist movements, particularly al-Queda, compare state-sponsored and

independent terrorist activities, and address the formidable problem of developing feasible counterterrorist measures and polices.

The value of these materials is both immediate and historical. They provide up-to-date information on the global war on terrorism, while documenting the manner in which terrorism has been perceived and addressed over more than three decades. These seminal studies are important now and will remain of value in the future.

REEL INDEX

The following is a listing of the folders comprising the microfilm publication entitled *Studies in Global Crisis: The Global War on Terrorism.* The Reel Index lists the frame number, folder title, as well as a listing of the major subjects for each folder.

REEL 1

Global War on Terrorism

0001 **Federal Bureau of Investigation, *Terrorism, 2001-2005,* U.S. Department of Justice, January 2006. 71pp.**

This edition of Terrorism highlights significant terrorism-related events in the U.S. and selected FBI investigative efforts overseas that occurred during the years 2002 through 2005. Additionally, this report provides a wide range of statistical data relating to terrorism in the United States during the past two decades. This material is presented to provide readers with an historical framework for the examination of contemporary terrorism issues.

0074 **Marburger, John H., III, *Combating Terrorism: Research Priorities in the Social, Behavioral and Economic Sciences,* National Science and Technology Council, January 2006. 23pp.**

The knowledge and tools of the social, behavioral and economic (SBE) sciences are immediately applicable to the construction of strategies that can enhance the Nation's capacity to predict, prevent, prepare for and recover from a terrorist attack. America's capacity to predict future terrorist attacks depends in part on the ability to identify and understand those factors that underlie the formation and maintenance of both domestic and international terrorist groups. Prediction capabilities are enhanced if we understand that terrorist networks and strategies are shaped by the behaviors of both the terrorists and their targeted adversaries, which differ across time, place, and access to resources. The ability to prevent a domestic terrorist attack will depend, in part, on detecting who threatens us. Behavioral methodology in conjunction with sensor and surveillance technology is being used to anticipate and detect threats during the earliest pre-incident phases.

0099 **Schweitzer, Glenn E. and A. Charles Sharber, *Countering Urban Terrorism in Russia and the United States,* National Academy of Science, January 2006. 252pp.**

This report presents the proceedings of the third U.S.-Russian inter-academy workshop on the general theme of countering terrorism. This report focuses on many important dimensions of urban terrorism, including the integration of response activities of different government organizations should a terrorist attack occur.

0354 **Office for Victims of Crime, *International Terrorism Victim Expense Reimbursement Program*, Office of Justice Programs, U.S. Department of Justice, February 2006. 26pp.**

Victims of acts of international terrorism occurring outside the U.S. often face unique obstacles in securing assistance, expense reimbursement, emergency transportation and short-term lodging, and appropriate medical and mental health care. Congress authorized the International Terrorism Victim Expense Reimbursement Program (ITVERP) to ensure that victims of international terrorism may receive reimbursement for their expenses associated with that Act. This OVC Report to Congress outlines the challenges and obstacles faced in developing ITVERP, details the groundwork laid thus far, and discusses the emergency assistance provided to victims in the interim while program regulations are being finalized.

0382 **Joint Chiefs of Staff, *National Military Strategic Plan for the War on Terrorism,* Department of Defense, February 1, 2006. 40pp**.

The NMSP-WOT constitutes the comprehensive military plan to prosecute the Global War on Terrorism (GWOT) for the Armed Forces of the U.S.. This document reflects the lessons of the first four years of the Global War on Terrorism, including the findings and commendations of the 9/11 Commission and a rigorous examination within the Department of Defense (DoD), personally led by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff. The NMSP-WOT outlines the Department's strategic planning and provides strategic guidance for military activities and operations in the GWOT. The document guides the planning and actions of the Combatant Commands, the Military Departments, Combat Support Agencies and Field Support Activities of the U.S. to protect and defend the homeland, attack terrorists and their capacity to operate effectively at home and abroad, and support mainstream efforts to reject violent extremism.

0422 **Cruz, Christopher A., *Look Out Below: Islamic Terrorism in South America,* Naval War College, February 13, 2006. 23pp**.

With hundreds of millions of dollars of financial support, ease of movement into the U.S. because of false passports and visas provided by corrupt South American government officials, and a sympathetic population filled with anti-American sentiment, the Islamic terrorist threat is very real in South America and should be a major security concern for the U.S. While U.S. Central Command (CENTCOM) receives most of the attention from U.S. political and military leaders due to the Global War on Terror (GWOT), the ongoing conflict in Iraq, and recent developments in Iran, the many threats in South America, to include Islamic terrorists, narco-terrorists, corrupt government officials, and the growing relationships among the three, is reason enough to elevate U.S. Southern Command (SOUTHCOM) from its current level of importance to one demanding the highest attention. In order to combat the growth of Islamic terrorism in South America, the U.S. must disrupt the conditions such as corruption, lawlessness, prevalence of drugs, and anti-Americanism that allow this terrorism to thrive.

0445 **Bolkcom, Christopher, and Batholomew Elias, *Homeland Security: Protecting Airliners from Terrorist Missiles*, Congressional Research Service, Library of Congress, February 16, 2006. 29pp**.

Recent events have focused attention on the threat that terrorists with shoulder fired surface-to-air missiles (SAMs), referred to as Man-Portable Air Defense Systems (MANPADS), pose to commercial airliners. Most believe that no single solution exists to effectively mitigate this threat. Instead, a menu of options may be considered, including installing infrared (IR) countermeasures on aircraft; modifying flight operations and air traffic control procedures; improving airport and regional security; and strengthening missile non-proliferation efforts. Equipping aircraft with missile countermeasure systems can protect the aircraft even when operating in areas where ground-based security measures are unavailable or infeasible to implement. However, this option has a relatively high cost, between 1 million and 53 million per aircraft, and the time needed for implementation does not allow for immediate response to the existing terrorist threat. Procedural improvements such as specific flight crew training, altering air traffic procedures to minimize exposure to the threat, and improved security near airports may be less costly than countermeasures and could more immediately help deter domestic terrorist attacks. However, these techniques by themselves cannot completely mitigate the risk of domestic attacks and would not protect U.S. airliners flying to and from foreign airports.

0474 **Sudnik, John, *"Dirty Bomb" Attack: Assessing New York City's Level of Preparedness from a First Responder's Perspective*, Naval Postgraduate School, March 2006. 120pp.**

Past history and recent intelligence have shown that New York City (NYC), a critical node of the U.S. economy, is clearly in the terrorist's crosshairs. In order to reduce the probability, lessen the risk, and minimize the consequences of a Radiological Dispersion Device (RDD), or dirty bomb, attack, NYC's first responders must be adequately prepared for its seemingly inevitable occurrence. This particular type of attack on NYC has the potential to create immense panic and confusion on behalf of the general public. Adding to the complexity of the problem is the notion that, since 9/11, the expected actions taken by employees in NYC high-rise office buildings in response to shelter-in-place instructions can be extremely difficult to predict. Therefore, a proposed public awareness campaign and a shelter-in-place plan are two cost-effective and easily implemented terrorism preparedness programs that would build the confidence and increase the capability of the citizenry. Since an RDD incident would likely result in a major inter-agency emergency operation, the unification of command, control, and coordination among NYC's first responder community is an essential element to its overall success. Hence, an informed and collaborative response by both public and private sector entities could potentially reduce casualties and save lives.

0592 **Kennedy-Boudali, Lianne, *The Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda*, Combating Terrorism Center, U.S. Military Academy, March 2006. 131pp.**

Faced with Western reactions to terrorist attacks on and after, 9/11, the Salfi Jihad movement has been forced to seek alternative methods to diffuse their ideas. One such medium, the internet, has given researchers and analysts at the Counter Terrorism Center the opportunity to thoroughly examine the role certain images and visual propaganda plays in the Jihadists' strategy. This study provides insight not only into how effective these images may be in

diffusing ideological ideas, but also offers use the ability to better understand what messages they may convey and what responses they may elicit. This understanding is critical in both how we formulate a response to counter Jihadists' growing influence, as well as understanding the threats we face. These images' value is beyond their simple visual aesthetics; rather they are often a carefully crafted element of an effective media campaign, designed to more widely offer the operational, tactical, and ideological education that once was available only in remote training camps.

0722 **Haque, M. Mahfuzul, *International Terrorism -- A War Without Boundary: Ways to Combat,* U.S. Army War College, March 15, 2006. 31pp**.

We live in an age of international terrorism with its ever-increasing reach and brutality. The nature and type of terrorism has become more varied and complex and terrorist organizations have become even more evasive and difficult to understand. There is a strong need to combat this hydra-headed monster of international terrorism. Counterterrorism tactics and tasks are often expensive and difficult. However, as yet there is no alternative to developing a strong and effective counterterrorism capability. Counterterrorism strategies and tactics must be developed by Democratic governments if they are to provide a measure of safety and security for their people and defeat terrorist organizations. This study will examine the nature and types of international terrorism; the threats posed by it; the characteristics of traditional terrorism (e.g., bombings, arson, assassinations, armed attacks, hostage-taking, kidnappings, sabotage) as compared with new terrorism (e.g., chemical, biological, radiological, nuclear, agricultural, and ecological terrorism, and cyber-terrorism); and the counterterrorism strategies that are needed to by Democratic states to combat international terrorism.

0753 **Brinkley, W. David, *Radical Theology as a Destabilizing Aspect of the 21st Century Strategic Security Continuum,* U.S. Army War College, March 15, 2006. 19pp.**

This study examines the role of radical theology and religious violence as destabilizing trends in the 21st Century. Radical religious ideology, or the corruption of a basic faith, enables widespread violence and destruction and elevates this type of terrorism to the strategic level. This paper reviews the basic definitions and causes of secular terrorism and then examines radical religious ideology using contemporary cases to study the organizational goals and fundamental beliefs of politically radical religious groups. From these cases' conclusions the potential threats and opportunities and a methodology are offered to identify, classify, and preempt or confront these types of adversaries. The study concludes with an analysis of religious terrorism's center of gravity and the vulnerabilities of this center of gravity, and with specific recommendations for U.S. decision makers.

0772 **Varinli, Mehmet, *Turkey's Crucial Contributions to the War Against Terrorism,* U.S. Army War College, March 15, 2006. 22pp.**

The first wave of modern political terrorism hit Turkey in 1925 and continued intermittently until 1971. The second stage of terrorism occurred between the years of 1975 and 1980. In 1979 -- nearly at the end of the Cold War -- the Kurdistan Worker Party (PKK) was founded. Turkey has been the main target of PKK-related terrorism. Although the Turkish Armed Forces have succeeded in fighting terrorism and preserving the country, the PKK has survived by becoming a transnational terrorist group and seeking refuge in nations neighboring Turkey. To solve the issue of transnational terrorism, all nations should reach a

consensus in this struggle and give a hand to each other. During the last three decades, the Turkish Armed Forces have gained a great deal of experience. Since the fall of the Iron Curtain, Turkey is and will remain an important partner for the U.S.. The purpose of this paper is to examine the U.S.-Turkey strategic partnership, the Turkish experience in the fight against terrorism, and the common security interest of the two countries. The paper also examines the two nations' war against terrorism through strategic alliance.

0794 **Doyle, Charles, *Material Support of Terrorists and Foreign Terrorist Organizations: Sunset Amendments in Brief*, Congressional Research Service, Library of Congress, March 17, 2006. 6pp**.

Section 6603 of the Intelligence Reform and Terrorism Prevention Act of 2004 amends two federal terrorist assistance prohibitions. This is an abbreviated version of CRS Report RL33035, Material Support of Terrorists and Foreign Terrorist Organizations: Sunset Amendments, without the footnotes, appendix, and some of the citations to authority found in the longer, parent report.

0800 **U.S. General Accountability Office, *Military Pay: Hundreds of Battle-Injured GWOT Soldiers Have Struggled to Resolve Military Debts*, U.S. General Accountability Office, April 2006. 31pp.**

Government Reform's continuing focus on pay and financial issues affecting Army soldiers deployed in the Global War on Terrorism (GWOT), the requesters were concerned that battle-injured soldiers were not only battling the broken military pay system, but faced blemishes on their credit reports and pursuit by collection agencies from referrals of their Army debts. GAO was asked to determine (1) the extent of debt of separated battle-injured soldiers and deceased Army soldiers who served in the GWOT, (2) the impact of DOD debt collection action on separated battle-injured and deceased soldiers and their families, and (3) ways that Congress could make the process for collecting these debts more soldier friendly.

0831 **Redd, John Scott, *National Strategy to Combat Terrorist Travel*, National Counterterrorism Center, May 2, 2006. 53pp.**

Constraining the mobility of terrorists is one of the most effective weapons in the War on Terror. Limiting their movements markedly diminishes terrorists' ability to attack the U.S., our interests abroad, or our allies. The 9/11 terrorist attacks highlighted the need to improve the monitoring and control of the domestic and international travel systems as a means to constrain terrorist mobility. Since then, the US Government has made considerable progress toward achieving this objective. The post-9/11 security environment consists of strengthened travel document security, enhanced screening of all visitors to the U.S., improved information-sharing relationships with foreign partners, and increased vigilance of the American people and our allies in the War on Terror. Our foreign partners have also made progress in strengthening border security and providing terrorist-related information to the U.S. in a timely and efficient manner.

REEL 2

Global War on Terrorism cont.

0001 **Hanley, John T., Jr., "The Anatomy of Terrorism and Political Violence in South Asia,"** ***Proceedings of the First Bi-Annual International Symposium of the Center for Asian Terrorism Research (CATR), October 19-21, 2005, Denpensar, Bali, Indonesia,*** **Institute for Defense Analyses, May 2006. 477pp.**

This document presents the proceedings of the First Bi-annual International Symposium of the Council for Asian Terrorism Research (CATR). The goals of the symposium, entitled The Anatomy of Terrorism and Political Violence in South Asia were threefold: to expand working relationships among scholars, analysts, journalists, and others with expertise in a variety of fields related to terrorism and political violence in the Southeast Asian region; to deepen formal cooperative and collaborative links between academic, analytical, and government institutions dealing with the problem of countering terrorism and extremist political violence; and to bring the broadest possible spectrum of knowledge and experience to bear on the problem to the mutual benefit of the all the institutions involved. The conference brought together academics, journalists, government experts, and military and law enforcement officers from across the region. The conference was organized into three thematic sessions: Interregional Fertilization of Political Violence and Terrorism, the Anatomy of Terrorism in South Asia, and IT and Terrorism.

0478 **International Business Legal Associates,** ***A Legal Study on Combating Money Laundry and Terrorism Finance under Jordanian Laws,*** **Office of Economic Opportunities, U.S. Agency for International Development/Jordan, June 2006. 20pp.**

Provides insights into legal advisory services regarding Money Laundry and Terrorism Finance in Jordan and the legal and regulatory framework provided under the Jordanian Laws for combating such acts within this concept.

0498 **Executive Office of the President,** ***National Strategy for Combating Terrorism,*** **Executive Office of the President, September 2006. 23pp.**

This updated strategy sets the course for winning the War on Terror. It builds directly from the National Security Strategy issued in March 2006 as well as the February 2003 National Strategy for Combating Terrorism, and incorporates an increased understanding of the enemy. From the beginning, we understood that the War on Terror involved more than simply finding and bringing to justice those who had planned and executed the terrorist attacks on September 11, 2001. The strategy involved destroying the larger al-Qaida network and also confronting the radical ideology that inspired others to join or support the terrorist movement. Since 9/11, we have made substantial progress in degrading the al-Qaida network, killing or capturing key lieutenants, eliminating safehavens, and disrupting existing lines of support. Through the freedom agenda, we also have promoted the best long-term answer to al-Qaida's agenda: the freedom and dignity that comes when human liberty is protected by effective democratic institutions.

0523 **U.S. General Accountability Office, *Foreign Assistance: Recent Improvements made, but USAID Should Do More to Help Insure Aid Is not Provided for Terrorist Activities in West Bank and Gaza,* U.S. General Accountability Office, September 29, 2006. 42pp.**

Analysis of recommendations to strengthen U.S. Agency for International Development's (USAID) efforts to help ensure that U.S. assistance to the West Bank and Gaza does not support terrorist activities, including addressing limitations with the USAID mission's vetting management database and developing antiterrorism policies and procedures for all its financial agreements.

0565 **Sanders, Deborah, *Ukraine After the Orange Revolution: Can It Complete Military Transformation and Join the U.S.-Led War on Terrorism?* Strategic Studies Institute, October 2006. 50pp.**

Ukraine can make two important contributions to the U.S.-led war on terror. It can consolidate its democracy and thereby be a force for peace and stability in the Eurasian region, and, second, through its military transformation, it can provide peacekeeping forces to zones of instability. In order to be an effective contributor to peacekeeping operations and to consolidate its democracy, Ukraine needs to engage in comprehensive military transformation. This will necessitate the reform of all security stakeholders--all those organizations responsible for the provision of security. Effective military transformation in Ukraine also will be dependent on the development of military professionalism, democratic political control, and democratic professionalism. Ukraine has made some notable progress in all these areas, though much remains to be done. Paradoxically, military transformation will make Ukrainian peacekeeping forces more deployable, but democratic consolidation is likely to place severe limits on how these forces are used in the future. In addition, Ukraine's desire for Euro-Atlantic integration also will speed up and add a qualitative element to Ukraine's military transformation, but this could damage relations with its largest neighbor, the Russian Federation, which could lead to the reemphasis of traditional definitions of defense rather than the development of niche capabilities.

0615 **Archick, Kristin, U.S.-EU *Cooperation Against Terrorism*, Congressional Research Service, Library of Congress, October 16, 2006. 6pp.**

The September 11, 2001, terrorist attacks gave new momentum to European Union (EU) initiatives to improve law enforcement cooperation against terrorism both among its 25 member states and with the U.S.. Washington has largely welcomed these efforts, recognizing that they may help root out terrorist cells and prevent future attacks. However, the U.S. and the EU continue to face several challenges as they seek to promote closer cooperation in the police, judicial, and border control fields.

0621 **McCants, William, *Militant Ideology Atlas: Executive Report*, Combating Terrorism Center, U.S. Military Academy, November 2006. 21pp**.

The Militant Ideology Atlas is the most recent and comprehensive attempt to better understand the ideology driving the Jihadi Movement. This Executive Report and its accompanying Research Compendium provide the first systematic mapping of the ideology driving the actions of the terrorists responsible for the 9/11 attacks and other violent actions around the world. Using a robust research methodology and critical analyses of the Jihadis'

most widely read texts, the Atlas gives us a highly nuanced map of the major thinkers in the Jihadi Movement and their most salient areas of consensus and disagreement. This Executive Report identifies who the most influential people are among the Jihadi thinking class, what they are thinking, and where the movement is most vulnerable ideologically. The report uses these empirical findings to identify powerful messages and influential messengers that can turn different constituencies against the Jihadis. These constituencies range from benign mainstream Muslims to the most violent Jihadis. The recommendations of this report establish a baseline against which strategic communications campaigns can be calibrated and adjusted. Appendix I is an Ideological Influence Map. Arrows indicate who is citing whom; thick lines are for an author who cites another author repeatedly; and the larger nodes indicate someone who is a key broker of information in the network. Appendix II is a listing of author names that have been cited three or more times in the Jihadi writings that were analyzed. The list is divided into modern authors and pre-modern authors. Each list includes the number of times the author has been cited, date of death, and nationality.

0642 **McCants, William, *Militant Ideology Atlas: Research Compendium*, Combating Terrorism Center, U.S. Military Academy, November 2006. 360pp.**

The Militant Ideology Atlas is the most recent and comprehensive attempt to better understand the ideology driving the Jihadi Movement. The empirically supported findings from this effort are generated by a systematic research methodology and critical analyses of hundreds of al-Qa`ida's most widely-read and influential texts. The wealth of information contained in the Atlas' Research Compendium provides a new generation of scholars and analysts with the data and evidence they need to understand America's adversaries and to devise strategies for combating them.

1001 **Cook, David, *Jihadi After Action Report: Paradigmatic Jihadi Movements*, Combating Terrorism Center, U.S. Military Academy, December 2006. 30pp**.

In January 2005, veteran jihadi thinker, propagandist, and historian Abu Musab al-Suri released his 1,600 page study of the jihadi movement, Dawat al-muqawama al- Islamiyya al-alamiyya (The Call for Global Islamic Resistance). Suri hoped this book would stimulate the creation of a comprehensive jihadi curriculum for future generations of jihadi fighters, thinkers, and activists who could learn from the mistakes and successes of jihads past. *In The Call*, Suri identifies twenty-five paradigmatic jihadi movements, or particularly edifying historical cases, where jihadis have both succeeded and failed to rally supporters, defeat their opposition, or establish territorial control. However, many of these jihadi movements are very obscure, and, consequently rarely studied within the Western counterterrorism community. In order to better appreciate the jihadi movement's strategic objectives and mindset, the Combating Terrorism Center invited David Cook, an expert on Islamic history and jihad, to provide deeper background on four of Suri's identified paradigmatic jihads: (1) experience of the Harakat al-Shabiba in Morocco (1969); (2) experience of the Harakat al-Dawla al-Islamiyya in Algeria (1982-1987); (3) The experience of the Afghani Arabs in Lebanon under Abu A'isha al Lubnani; and (4) The experience of the Islamic Army of Aden Abyan in Yemen during the 1990s. Despite the factual errors Cook identifies throughout Suri's work, the latter's stature in the jihadi movement means that future jihadis will take his analysis seriously and model their strategies accordingly.

1032 **Ulph, Stephen, *Jihadi After Action Report: Syria*, Combating Terrorism Center, U.S. Military Academy, December 2006. 19pp.**

Despite its crackdown on the Muslim Brotherhood in the early 1980s, the Asad regime has had to contend with a rising tide of Islamist activity due, in part, to its pandering to the Sunni religious establishment to shore up its legitimacy. However, the growing appeal of Islamism (the notion that Islam should be the primary source of law and identity in Muslim-dominated countries) has made it more difficult for the Jihadis to attract a large following. This is due to the following factors: (1) the Jihadis' uncompromising puritanism, which makes their ideology religiously repugnant and prevents them from engaging in pragmatic political actions and alliances; (2) the Jihadis' lack of scholarly firepower, which makes it hard for them to stand up to government-sponsored clerics and justify their cause and their violent tactics to the masses; (3) improved security measures in the past year; (4) the infiltration of Jihadi groups by clerics; (5) the influence of Sufism (Islamic mysticism); (6) popular televangelists that preach tolerance and pacifism; (7) the willingness of popular Islamist groups like Hamas and Hizbullah to participate in democratic elections; (8) competing identities, either ethnic (e.g., Kurds), sectarian (e.g., Alawite, Shia, Christian, Druze), or nationalist; and (9) the pull of Western culture, particularly among the youth.

1051 **Aboul-Enein, Youssef, *Egyptian Collection on Islamist Militant Groups: Expose of the Writings of Terrorism Scholar Abd al-Raheem Ali on al-Qaida*, Combating Terrorism Center, U.S. Military Academy, December 2006. 12pp.**

The examination of what Arab scholars and commentators are saying about the problem of violent Islamist militancy has become an important yet neglected part in the education of future American military leaders. The Joint Forces Command has started the process with its three-volume *Terrorism Perspectives Project* that provides insight into such al-Qaida thinkers as Abu Musab al-Suri, the Clausewitz of al-Qaida-affiliated networks.

1063 **Martin, Elizabeth, *"Terrorism" and Related Terms in Statute and Regulation: Selected Language*, Congressional Research Service, Library of Congress, December 5, 2006. 5pp**.

Congress has used the term terrorism often in legislation. Hundreds of federal statutes and regulations already refer to terrorism and related terms in a variety of other contexts. However, these statutes and regulations ultimately refer to an extremely small set of statutory definitions, current criminal law and immigration definitions among them. This report provides the current text of a few of the fundamental definitions.

REEL 3

Global War on Terrorism cont.

0000 **Macdonald, Douglas J., *The New Totalitarians: Social Identities and Radical Islamist Political Grand Strategy,* Strategic Studies Institute, January 2007. 88pp.**

Academic and journalistic critics of the American Long War on Terrorism (LWT) who are calling for negotiations with radical Islamist groups, to attempt to appease such groups by meeting their allegedly limited demands, or to accept that they do not represent a major threat to the U.S. and its interests, are fundamentally wrong. There are many reasons for this, but the major flaw in such reasoning is a lack of understanding of the ideologically-driven grand political strategy of the Islamist extremists, which represents a totalitarian, transnational, and, in many versions, universalist social revolutionary movement. Moderate rationalists have difficulty understanding the rigidity of historical necessity or moral imperatives in the totalitarian mindset. Policy advice that flows from such misunderstanding is therefore fatuous, if not dangerous. A proper understanding of the grand political strategy chosen by the terrorists is a prerequisite for constructing effective counter policies. Dr. Macdonald argues that the first thing to understand about the enemy is that there is nothing to negotiate with them because of their radical totalitarian nature. The debate over grand strategy in the Long War on Terrorism is a robust one. Dr. Macdonald's use of social identity theory to provide a framework to understand the terrorist enemy and how to deal with him moves that debate forward.

0091 **Office of Foreign Assets Control, *Terrorist Assets report, Calendar Year 2006,* Department of Treasury, January 2007. 19pp**.

Section 304 of Public Law 102-138, as amended by Public Law 103-236 (22 U.S.C. § 2656g) (hereinafter referred to as Section 304) (Tab 1), requires the Secretary of the Treasury, in consultation with the Attorney General and appropriate investigative agencies, to provide an annual report to the Congress concerning the nature and extent of assets held in the U.S. by terrorism-supporting countries and organizations engaged in international terrorism. The Department of the Treasury submitted its first Terrorist Assets Report to the Congress in April 1993. The current report, covering calendar year 2006, is the fifteenth successive Terrorist Assets Report.

0110 **Perl, Raphael F., *International Terrorism: Threat, Policy, and Response,* Congressional Research Service, Library of Congress, January 3, 2007. 35pp.**

This report examines international terrorist actions, threats, U.S. policies and responses. It reviews the nation’s use of tools at its disposal to combat terrorism, from diplomacy, international cooperation, and constructive engagement to physical security enhancement, economic sanctions, covert action, and military force.

0145 **Morris, Grant L.,** ***A New Kind of War: Are We Prepared for Agroterrorism?*** **School of Advanced Military Studies, Command and General Staff College, January 5, 2007. 56pp.**

The American agricultural industry produces the world's safest and cheapest food, but those systems which make the industry so reliable also make it vulnerable. Individuals who desire to disrupt the U.S. economy could introduce a small quantity of plant or animal pathogens into the many unprotected nodes of the agricultural system creating the most devastating attack the U.S. has ever seen. Providing 13% of the U.S. Gross Domestic Product (GDP), employing 15% of the U.S. population and producing more than $50 billion yearly in exports, agriculture is one of the primary industries in the U.S. and one of the few industries with a positive trade balance. Although a single attack on the agricultural industry may not result in its destruction, an attack would result in the interruption of food supplies, disruption of interstate travel and trade embargos placed on the U.S. The psychological impacts of a major agroterrorist attack would be similar to the impact 9/11 had on the airline industry.

0201 **Mitra, Durga Madhab (John),** ***Understanding Indian Insurgencies: Implications for Counterinsurgency Operations in the Third World,*** **Strategic Studies Institute, February 2007. 84pp.**

The objective of this paper is to develop a theoretical perspective for analyzing the Indian experience with insurgency, and to discuss its implications for counterinsurgency in Third World countries. Understanding the affected population is essential for understanding an insurgency or planning for counterinsurgency. The contested population is not only the end; it is also an important means for the insurgent. The insurgents and government of the day compete with one another to control the population, as well as to gain the populace's loyalty.

0285 **Aiken, Scott D.,** ***Department of Defense Sponsorship of "Soft Power" in Support of the Global War on Terrorism,*** **Air War College, February 23, 2007. 46pp.**

The Global War on Terrorism (GWOT) is a struggle of numerous, ever changing dimensions. One dimension currently the scene of a complex, massive battle is the information domain, a "War of Ideas." The U.S. has gained advantage in this domain by strengthening deliberately its "soft power." As a premier US Government agency in the GWOT, the Department of Defense (DOD) has added soft power to its arsenal.

0331 **Gross, Max L.,** ***A Muslim Archipelago: Islam and Politics in Southeast Asia,*** **National Defense Intelligence College, March 2007. 296pp.**

Southeast Asia continues to beckon policymakers and scholars alike to revisit its history in spite of the tomes of appraisals already written, deconstructive or otherwise. Because of a significant presence of Muslims in the region, and particularly in the wake of 9/11, it invariably attracts the attention of foreign powers drawn by the specter of terrorism and focused on rooting out radical Islamist groups said to be working with al-Qaeda.

0627 **Ball, John E.,** ***Rethinking Intelligence to Integrate Counterterrorism into the Local Law Enforcement Mission,*** **Naval Postgraduate School, March 2007. 109pp.**

Law enforcement agencies are constantly challenged by a changing threat environment, and they attempt to meet the challenges with the resources they have. In the past twenty years, terrorism is a dangerous threat to America while community expectations to address crime have also grown. Americans rely on local, state, and federal law enforcement to understand this threat and to incorporate counter terrorism efforts into their already full missions.

0736 **Leavell, Ron,** ***The Evolution of Regional Counterterrorism Centers Within a National Counterterrorism Network: Is It Time to Fuse More Than Information?*** **Naval Postgraduate School, March 2007. 153pp.**

There is widespread consensus among both policymakers and intelligence professionals that domestic counterterrorism efforts remain hampered by the lack of an effective national intelligence network that fully integrates the Homeland's entire intelligence assets and other related Homeland Security capabilities into one national counterterrorism system. The failure to unify domestic counterterrorism efforts inhibits timely and complete information sharing and the evolution of a more robust Homeland Security prevention and response capacity.

0891 **Morrissey, James F.,** ***Strategies for the Integration of Medical and Health Representation Within Law Enforcement Intelligence Fusion Centers,*** **Naval Postgraduate School, March 2007. 92pp.**

Terrorism-related intelligence gathering, analysis and information dissemination would be improved and enhanced by including a medical and health element in law enforcement intelligence fusion centers. The lack of medical representation and participation in intelligence analysis and information dissemination has been an obstacle to effective terrorism prevention, preparedness and response. Terrorist acts, including weapons of mass destruction, would have a significant and profound impact on the medical and health community.

0985 **Aboul-Enein, Toussef,** ***Sheikh Abdel-Fatah Al-Khalidi Revitalizes Sayid Qutb: Inside the Adversary's Anti-American Ideology from the Cold War to Operations Iraqi Freedom,*** **Combat Terrorism Center, U.S. Military Academy, March 2007. 11pp.**

This article highlights a recent booklet published by radicalist cleric Sheikh (Dr.) Salah Abdel-Fatah Al-Khalidi entitled “Al-Harb Al-Amriki bee Manather Sayid Qutb (The American War from the Perspective of Sayid Qutb).” The booklet is unique because it both revives Qutb’s writings four decades after his death and concentrates all of Qutb’s hatred and vitriolic ideology specifically directed against the U.S..

0996 **Fishman, Brian,** ***Fourth Generation Governance: Sheikh Tamini Defends the Islamic State of Iraq,*** **Combat Terrorism Center, U.S. Military Academy, March 23, 2007. 11pp.**

On October 15, 2006 Al-Qa’ida in Iraq (AQI) and its allies declared an independent Islamic State across a swath of Western Iraq. The Islamic State of Iraq (ISI) was widely scorned by Western counterterrorism experts, many of whom rightly concluded that the ISI would never

be capable of developing the material and bureaucratic infrastructure widely expected of a modern state.

1007 **Jaradet, Mohammad S.,** ***The Terrorism Threat and Countering Terrorism from Jordanian Perspective,*** **U.S. Army War College, March 30, 2007. 21pp.**

Terrorism remains a source of concern for all those who yearn to live in stability and peace. Jordan has experienced different kinds of terrorism throughout the last few decades, and its experience may provide important insights into the best ways to fight terrorism. This paper focuses on terrorism as an internal and external threat in Jordan. The following topics are examined: the strategic environment (international, regional, and local) and terrorism; the most important terrorism issues affecting Jordanian national security; and policies and strategies Jordan is applying to counter terrorism. As part of the discussion, the author analyzes the Amman Message of November 2004, which addressed the misunderstanding that exists about the connection between Islam and Muslim extremism.

1028 **Bueno de Mesquita, Ethan,** ***Correlates of Public Support for Terrorism in the Muslim World,*** **U.S. Institute of Peace, May 17, 2007. 51pp.**

This report examines the correlates of individual-level support for terrorism in fourteen Muslim countries and identifies a variety of factors that are correlated with support for terrorism. These factors can be divided into a several categories: attitudes toward Islam, attitudes toward the U.S., attitudes toward politics and economics in the home countries, and demographic factors.

REEL 4

Global War on Terrorism cont.

0001 **Barbosa, Adriano M.,** ***Combating Terrorism in the Brazilian Tri-Border Area: A Necessary Law Enforcement Strategic Approach,*** **Naval Postgraduate School, June 2007. 78pp.**

In the Brazilian Tri-border Area (TBA) terrorism has its own characteristics. In the TBA, terrorist groups are focused on supporting activities for their organizations. The problems related to terrorism in the TBA are connected with the struggle between Arabs and Israelis in the Middle East. Terrorist groups, such as Hezbollah and HAMAS, have operatives in the TBA in order to raise money and provide logistics to support their groups. In addition, these supporting activities are, as a rule, criminal efforts. So in the TBA, the best statecraft instrument to combat terrorism is law enforcement. In the Triple Frontier crime is the center of gravity for terrorism, and, as a consequence, the police are the most capable agency to deal with this situation. They can better prosecute organizations that perpetrate crimes to support terrorist groups. Hence, Brazil, Argentina and Paraguay must develop a strategic law enforcement approach to combat terrorism, based on ends, ways and means, with emphasis on police intelligence operations and covert criminal investigations.

0078 **Al-Hajjri, Ibrahim, *The New Middle east Security Threat: The Case of Yemen and the GCC,* Naval Postgraduate School, June 2007. 87pp.**

Since Yemen has a history of border disputes with Saudi Arabia, this addresses the question of Yemen's role in the security of the Arabian Peninsula. Yemen suffers from a weak economy and a number of security issues of its own. Through the borders shared with its GCC neighbors, Yemen has become plagued by a nexus of terrorism, arms smuggling, and drug trafficking. Yet Yemen is unable to effectively combat these threats because of weak border control and poor cooperation with its regional neighbors, which points to the issues of border control and transnational cooperation within the GCC as an important area of research.

0165 **Self, Kevin A., *Counterterrorism Policy in Colombia,* Naval Postgraduate School, June 2007. 76pp**.

The purpose of this thesis is to suggest a coherent, credible, and long-term counterterrorism policy in Colombia. The events of September 11, 2001 heightened U.S. awareness of Colombian terrorist organizations, the most powerful being the Revolutionary Armed Forces of Colombia (FARC). The U.S. counter-terror approach in Colombia appears fragmented, with only minor changes to its previous drug control policies. In contrast, the Colombian government has developed and implemented a policy to combat the FARC. To analyze the effectiveness of the Colombian government's efforts, this thesis takes a two-step approach.

0242 **Office of the Director of National Intelligence, *The Terrorist Threat to the U.S. Homeland,* National Intelligence Council, July 2007. 7pp.**

Consists of analytical judgments of the intelligence community regarding the likely course of future terrorist threats and attacks on the U.S. homeland.

0249 **Bowman, M. E., *Counterterrorism Activities of the FBI: At Home and Abroad,* Office of the Deputy Assistant Secretary of Defense & National Defense University, August 2007. 19pp**.

It was in Afghanistan where the utility of law enforcement expertise and techniques in a conflict zone first became evident. Prior to the terrorist attacks of 9/11, the FBI, and more specifically the New York Field Office, was the single most complete repository of information about Al Qaeda. Two New York Field Office agents were deployed to Bagram Air Force Base where their knowledge of Al Qaeda organization, personnel, and modus operandi quickly became invaluable in helping military forces to understand what and who they were confronting, both on the battlefield and in detention facilities.

0268 **Parker, Michelle, *Programming Development Funds to Support a Counterinsurgency: A Case Study of Nangarhar, Afghanistan in 2006,* Office of the Deputy Assistant Secretary of Defense & National Defense University, August 2007. 24pp.**

This case study describes one method of programming development funds at a sub-national level to positively affect a counterinsurgency in Eastern Afghanistan. It is presented as a

practical model for both students in the classroom and operators in the field to understand the complexity involved with a type of mission that the U.S. has not attempted since Vietnam. The case study explores the process through which the Jalalabad Provincial Reconstruction Team (PRT) developed and implemented a strategy for increasing stability in its area of operations through maximizing resources each agency brought to the table and creating a "unity of effort."

0292 **U.S. Army, *U.S. Army TRADOC Handbook: A Military Guide to Terrorism in the Twenty-First Century*, U.S. Army Training and Doctrine Command, Fort Leavenworth, August 15, 2007. 182pp.**

Understanding terrorism spans foreign and domestic threats of nation-states, rogue states with international or transnational agents, and other actors with specific strategies, tactics, and targets. This guide, prepared under the direction of the U.S. Army Training and Doctrine Command (TRADOC) and the TRADOC Intelligence Support Activity (TRISA)-Threats, addresses foreign and domestic threats against the U.S. of America in a contemporary operational environment (COE). Compiled from open source materials, this handbook promotes a 'Threats' perspective and enemy situational awareness of U.S. strategies and operations in combating terrorism. Neither a counterterrorism directive nor antiterrorism manual, this handbook complements but does not replace Army training and intelligence products on terrorism. This handbook exists primarily for U.S. military forces.

0474 **U.S. Army, *U.S. Army TRADOC Handbook: Terrorism and WMD in the Contemporary Operational Environment*, U.S. Army Training and Doctrine Command, Fort Leavenworth, August 20, 2007. 166pp**.

Supplemental handbook to the U.S. Army TRADOC G2 Handbook No. 1, A Military Guide to Terrorism in the Twenty-First Century. The capstone reference guide describes terrorism and its potential impacts on U.S. military forces in the conduct of mission operations. This supplemental handbook highlights the nature of terrorism present in a full spectrum contemporary operational environment (COE) and terrorist intentions to use weapons of mass destruction. Terrorist intent to obtain and use weapons of mass destruction (WMD) is one of the most serious contemporary threats to our Nation. The threat of WMD terrorism to the U.S. is present across the entire spectrum of conflict. Potential exists for WMD terrorism with individual acts of wanton damage or destruction of property or person, as well as operations conducted by organized violent groups or rogue states with social, environmental, religious, economic, or political agendas.

0637 **Terrill, W. Andrew, *Kuwaiti National Security and the U.S.-Kuwaiti Strategic Relationship After Saddam*, Strategic Studies Institute, September 2007. 116pp.**

This monograph provides a comprehensive and nuanced examination of Kuwait defense and security issues including a consideration of the importance of the current security relationship with the U.S.

0753 **Zuhur, Sherifa, *Egypt: Security, Political, and Islamist Challenges*, Strategic Studies Institute, September 2007. 161pp.**

This monograph addresses three issues in contemporary Egypt: failures of governance and political development, the continued strength of Islamism, and counterterrorism. It is easier to tackle their contours in Egypt if they are considered separately. They are not, however, separate or independent; continuing to treat them as mutually exclusive conditions will lead to further crisis down the road. Egyptian failures of governance have taken place through three eras: monarchy and the liberal experiment, the period of Arab socialism, and Egypt's reopening to the West under Presidents Sadat and Mubarak.

0914 **Reveron, Derek S., *Shaping the Security Environment*, Naval War College, September 2007. 113pp.**

This paper makes an important contribution to an unfolding debate on the global role of U.S. military forces in an era of transnational terrorism, failed or failing states, and globalization. The paper looks beyond the current conflicts in which the U.S. is involved to raise fundamental questions concerning the regional diplomatic roles of America s combatant commanders (COCOMs) and, more generally, the entire array of non-warfighting functions that have become an increasingly important part of the day-to-day life of the American military as it engages a variety of partners or potential partners around the world. These functions are increasingly being given doctrinal definition and a larger role in U.S. military planning under the novel concept of shaping. This volume is intended to explore the notion of shaping in its various aspects, both generally and in several regional contexts.

1026 **Zabel, Sarah E., *The Military Strategy of Global Jihad*, Strategic Studies Institute, October 2007. 23pp.**

America entered the Global War on Terrorism with little understanding of the enemy it faced. Al-Qaeda plays a leading role in the larger movement of global jihad, a splinter faction of militant Islamism intent on establishing its vision of strict Islamic rule in the Muslim world through armed action. Global jihadis have spent more than 40 years refining their philosophy, gaining experience, building their organization, and developing plans to reestablish what they see as the only true Islamic state on earth. The September 11, 2001 attacks set this plan in motion. In the years leading up to and following the 9/11 attacks, global jihadis have written copiously on their military strategy for creating an Islamic state. This paper draws on those writings to examine and explain the mechanisms by which they plan to neutralize the superpower guardian of world order, claim land and peoples for Islamic emirates out of the resulting chaos, and bring these emirates together to become a true Islamic state. Their writings also expose weaknesses in their strategy, and this paper explores some of those potential vulnerabilities as well.

1049 **Dobrot, Laurence Andrew, *The Global War on Terrorism: A Religious War?* Strategic Studies Institute, November 2007. 24pp.**

The U.S. has been actively engaged in prosecuting the Global War on Terrorism (GWOT) since September 2001. However, after five years of national effort that has included the loss of over 3,000 service members in combat operations, many question whether the U.S. strategy is working and whether the U.S. understands how to combat an enemy motivated by

a radical revolutionary religious ideology. This Strategy Research Project (SRP) reviews the pertinent cultural history and background of Islam and then posits three root causes of this conflict: the lack of wealth-sharing in Islamic countries, resentment of Western exploitation of Islamic countries, and a U.S. credibility gap within the Islamic community. Following this discussion of root causes, this analysis compares the Ends, Ways and Means of the U.S. Strategy for Combating Terrorism with that of terrorist organizations such as Al Qaeda. This SRP concludes that the U.S. is not achieving its long term strategic objectives in the GWOT.

REEL 5

Global War on Terrorism cont.

0001 **Woods, Kevin M.,** ***Iraqi Perspectives Project: Saddam and Terrorism: Emerging Insights from Captured Iraqi Documents, Volume 1,*** **Joint Advanced Warfighting Program, Institute for Defense Analyses, November 2007. 94pp.**

Captured Iraqi documents have uncovered evidence that links the regime of Saddam Hussein to regional and global terrorism, including a variety of revolutionary, liberation, nationalist, and Islamic terrorist organizations. While these documents do not reveal direct coordination and assistance between the Saddam regime and the al Qaeda network, they do indicate that Saddam was willing to use, albeit cautiously, operatives affiliated with al Qaeda as long as Saddam could have these terrorist operatives monitored closely. Because Saddam's security organizations and Osama bin Laden's terrorist network operated with similar aims (at least in the short term), considerable overlap was inevitable when monitoring, contacting, financing, and training the same outside groups. This created both the appearance of and, in some ways, a "de facto" link between the organizations. At times, these organizations would work together in pursuit of shared goals but still maintain their autonomy and independence because of innate caution and mutual distrust. Though the execution of Iraqi terror plots was not always successful, evidence shows that Saddam's use of terrorist tactics and his support for terrorist groups remained strong up until the collapse of the regime.

0095 **Woods, Kevin M.,** ***Iraqi Perspectives Project: Saddam and Terrorism: Emerging Insights from Captured Iraqi Documents, Volume 2,*** **Joint Advanced Warfighting Program, Institute for Defense Analyses, November 2007. 560pp**.

0654 **Woods, Kevin M.,** ***Iraqi Perspectives Project: Saddam and Terrorism: Emerging Insights from Captured Iraqi Documents, Volume 3,*** **Joint Advanced Warfighting Program, Institute for Defense Analyses, November 2007. 448pp**.

REEL 6

Global War on Terrorism cont.

0001 **Woods, Kevin M.,** ***Iraqi Perspectives Project: Saddam and Terrorism: Emerging Insights from Captured Iraqi Documents, Volume 4,*** **Joint Advanced Warfighting Program, Institute for Defense Analyses, November 2007. 455pp**.

0456 **Woods, Kevin M.,** ***Iraqi Perspectives Project: Saddam and Terrorism: Emerging Insights from Captured Iraqi Documents, Volume 5,*** **Joint Advanced Warfighting Program, Institute for Defense Analyses, November 2007. 470pp.**

0926 **Berschinski, Robert G.,** ***AFRICOM's Dilemma: The Global War on Terrorism, Capacity Building, Humanitarianism, and the Future of U.S. Security Policy in Africa,*** **Strategic Studies Institute, November 2007. 77pp**.

The February 2007 decision to launch a new Department of Defense Unified Combatant Command for Africa (AFRICOM) was met with significant controversy both in the U.S. and abroad. AFRICOM's proponents claimed that the new command accurately reflected Africa's growing strategic importance and an enlightened U.S. foreign policy focused on supporting African solutions to African problems. Its critics alleged that the command demonstrated a self-serving American policy focused on fighting terrorism, securing the Africa's burgeoning energy stocks, and countering Chinese influence.

REEL 7

Global War on Terrorism cont.

0001 **Wrona, Richard M.,** ***A Deafening Silence: Hizballah After the American Invasion of Iraq,*** **Combat Terrorism Center, U.S. Military Academy, November 2007. 47pp.**

In 1983, the U.S. became intimately familiar with Hizballah and the ramifications of international terrorism. In April, a Hizballah member, using a previously unseen tactic, drove a truck laden with explosives into the American Embassy in Lebanon, killing sixty-one people. Then in October, in well-planned, simultaneous operations, suicide bombers using the same method struck the barracks complexes of American and French peacekeepers, killing two hundred forty-one American servicemen and twenty-three French soldiers. Following September 11th, 2001, the U.S. marked Hizballah one of the primary targets of the GWOT. Although al Qaeda and its affiliates were responsible for the most recent attacks against U.S. interests, many government officials and terrorism experts rank Hizballah as the greatest threat to American interests and security, particularly interests in the Middle East.

0048 **Russell, James A.,** ***Regional Threats and Security Strategy: The Troubling Case of Today's Middle East,*** **Strategic Studies Institute, November 2007. 56pp.**

Like the Arab-Israeli Six-Day War of 1967, the U.S. invasion of Iraq is fundamentally reordering regional politics and security in ways that will be felt for a generation, if not longer. The Pandora's Box opened by the U.S. in Iraq adds a new level of unwelcome complexity to an already strained regional fabric. Threats to regional security stem from global, interstate, and intrastate sources. The complicated, multidimensional, and interrelated natures of these threats suggest that the U.S. must reassess strategy and policy if it is to protect and further its regional interests. The objective of this monograph is threefold: (1) deconstruct the threats to regional security and stability in the aftermath of the Iraq invasion;

(2) determine whether U.S. strategy is tailored to the threat environment; and (3) suggest steps that can be taken to bring strategy and the environment into closer alignment.

0104 **Gooding, Aeneas R., *Agricultural Terrorism (Agroterror) and Escalation Theory,* Naval Postgraduate School, December 2007. 93pp.**

The debate about whether sub-state actors have an interest in conducting a WMD attack using chemical or biological weapons is embedded within escalation theory, which holds that in order to maintain credibility terrorist groups must demonstrate a continued ability to conduct operations and inflict significant numbers of casualties on their enemy, maintaining a consistent, if not escalating level of violence. This thesis uses E. coli in produce and foot and mouth disease in livestock case studies to evaluate U.S. systems' ability to contain such an agroterror attack and to estimate likely results of such attacks. The analysis shows that neither an FMD attack on livestock nor an E. coli attack on produce is likely to cause sufficient casualties, economic disruption, and/or fear and panic to constitute escalation from recent conventional attacks for an established international terrorist organization. Therefore, agroterror attacks are not likely to be particularly attractive for such organizations.

0197 **McAlexander, Joseph C., IV, *Hearts and Minds: Historical Counterinsurgency Lessons to Guide the War of Ideas in the Global War on Terrorism,* Air University, December 2007. 43pp.**

To address the potential terrorist threats to America, the U.S. National Security Strategy and the National Strategy for Combating Terrorism state that the U.S. will wage a “war of ideas.” The war of ideas seeks to change the minds of varying ideological populations. A war fought in the minds and among people -- human terrain -- requires human players to engage and communicate with indigenous populations in the context of the local culture. As the U.S. and its coalition partners in the global war on terror (GWOT) clear al-Qaeda from one location, terrorists will seek other locations. They target people to turn them against the U.S. and the coalition of the willing. A foreign or local government can win the war of ideas and defeat global terrorists only if it wins the hearts and minds of the people, which requires influencing their behavior by offering them a better solution than the solution al-Qaeda offers. A war of ideas is not new to the twenty-first century fight. While history cannot provide a panacea for global terrorism, today's military can learn lessons from historical small wars and low intensity conflicts to train and employ forces effectively to wage and win a war of ideas to counter global insurgents and their ability to win popular support. This paper employs a review of two case studies, Malaya (1945-60) and Vietnam (1964-72).

0240 **Heffelfinger, Chris, *Trends in Egyptian Salafi Activism,* Combat Terrorism Center, U.S. Military Academy, December 2007. 17pp.**

This report will explore the status of radical Islamic ideology and its popularity among Egyptians in Cairo. It stems in part from an October 2007 research trip to gain insights into Salafi-jihadi activism and the political, social and religious climate that either supports or inhibits its growth. That climate in Cairo gauged by recent public opinion polls, my interviews and observations, and trends among Salafis in Egypt today does not seem to bode favorably for militant Islamist activism. The city is not a center for this ideology or its movement, partly due to recent economic success, belief in democratic principles and Egyptian Muslims' rejection of violent tactics. Egypt served as the wellspring for modern

Islamism and has had more than a century of evolving Salafi thought and activism. Certainly, foreign-born Muslims and Egyptians alike are well aware of this country's and especially Cairo's unique place in contemporary Muslim thought. It has produced some of the most influential Islamist thinkers and organizers of recent history Muhammad Abduh, Rashid Rida, Hasan al-Banna and Sayyid Qutb who collectively dealt with issues of Islamic reform and revivalism, modeled on Salafi ideals. In recent decades, it has also produced or trained leading jihadi figures such as Ayman al-Zawahiri, Abdullah Azzam, and Umar Abd al-Rahman. The Islamist movement, greatly weakened by crackdowns in the late 1990s, does not pose the same threat it once did to the Egyptian state. The tension between the city's towering Islamist past and the newfound sense of progress and prosperity creates a duality in Egypt's capital that, for the time being, is a positive sign for U.S. efforts to combat terrorism. That is, there is for many a coexistence of Islam and Egyptian nationalism, which is open to the West and often associated with democratic values.

0257 **Flanagan, Stephen J., and James A Schear, *Strategic Challenges: America's Global Security Agenda,* National Defense University, December 2007. 425pp.**

This volume presents a trenchant analysis of seven major national security challenges that the U.S. will confront in the coming decade, including countering global terrorism; combating the threats posed by the proliferation of mass destruction weapons; protecting the American homeland; defusing conflicts in unstable regions; engaging other major powers; adapting alliances and partnerships; and transforming the U.S. defense strategy and military posture. The authors provide a cogent and balanced evaluation of the progress made, and pitfalls encountered, in addressing these challenges since 2001. They then advance a set of practical strategy and policy options for consideration by future administrations. The final chapter presents a synthesis of the entire book and integrated strategy for managing American security in this volatile period.

0682 **Kumar Arvind, and Roddam Narasimha, *Science and Technology to Counter Terrorism: Proceedings of an Indo-U.S. Workshop,* National Academy of Science, December 2007. 178pp.**

This volume presents the papers and summarizes the discussions of a workshop held in Goa, India, in January 2004, organized by the Indian National Institute of Advanced Science (NIAS) and the U.S. Committee on International Security and Arms Control (CISAC). During the workshop, Indian and U.S. experts examined the terrorist threat faced in both countries and elsewhere in the world, and explored opportunities for the U.S. and India to work together. Bringing together scientists and experts with common scientific and technical backgrounds from different cultures provided a unique opportunity to explore possible means of preventing or mitigating future terrorist attacks.

0862 **Dunn, Lewis A., *Next Generation Weapons of Mass Destruction and Weapons of Mass Effects Terrorism,* Advanced Systems and Concepts Office, Defense Threat Reduction Agency, January 2008. 214pp.**

REEL 8

Global War on Terrorism cont.

0001 **Office of Foreign Assets Control, *Terrorist Assets Report, Calendar 2007*, U.S. Department of the Treasury, January 2008. 18pp.**

The Department of the Treasury's Office of Foreign Assets Control (OFAC) is the lead office for implementing sanctions with respect to assets of international terrorist organizations and terrorism-supporting countries. OFAC implements these sanctions as part of its general mission to administer and enforce economic and trade sanctions based on U.S. foreign policy and national security goals. In administering and enforcing U.S. economic sanctions programs, OFAC focuses on identifying persons for designation; assisting U.S. persons in complying with the sanctions prohibitions through its compliance and licensing efforts; assessing civil monetary penalties against U.S. persons violating the prohibitions; working with other U.S. Government agencies, including law enforcement; and coordinating and working with other nations to implement similar strategies. Currently, OFAC administers sanctions programs targeting international terrorists and terrorist organizations. OFAC also administers sanctions programs relating to the five countries that have been designated as state sponsors of terrorism.

0019 **Smith, James M., et al., *Strategic Culture and Violent NonState Actors: Weapons of Mass Destruction and Asymmetrical Operations Concepts and Cases,* Institute for National Security Studies, U.S. Air Force Academy, February 2008. 101pp**.

This occasional paper combines three separate threads of analysis on culture and violent non-state actors as a launching pad to spur further research into this critical arena of culture and security. In the first contribution, "Strategic Culture and Violent NonState Actors: Concepts and Templates for Analysis," James M. Smith lays out a conceptual basis and a series of templates for guiding the analysis of culture and violent non-state actors. These templates focus on the analysis of WMD acquisition and use, and on culturally driven operational campaigns. In the second contribution, "Strategic Culture, Al Qaida, and Weapons of Mass Destruction," Jerry M. Long applies a cultural analysis of radical Islam and al Qaida in discussing the many factors and influences involved in the core al Qaida group's WMD decisions. His work graphically demonstrates the complexity of such decisions for that core group, and suggests that what many may find as counter-intuitive caution plays a major role here. In the final contribution, "The Taliban Insurgency and Its Tribal Dynamics: An Analysis of 'Shabnamah' (Night Letters)," Thomas H. Johnson, in examining a tribal insurgent psychological campaign in Afghanistan, demonstrates that traditional beliefs, myths and stories, and behavioral influences can be manipulated for significant effect in countering U.S. efforts to gain stability and legitimacy for the Afghan government. Together these papers underscore the central role of culture in analyzing and understanding non-state adversaries.

0121 **Kan, Paul Rexton, *Drug Intoxicated Irregular Fighters: Complications, Dangers, and Responses,* Strategic Studies Institute, March 2008. 50pp.**

The complexity of many ongoing and persistent conflicts in the post-Cold War is partially attributed to the widespread presence of drug intoxicated irregular fighters. Drug consumption in contemporary wars has coincided with the use of child soldiers, has led to increased unpredictability among irregular fighters, provided the conditions for the breakdown of social controls and commission of atrocities, and caused the lessening of command and control among the ranks. Although the nonmedical use of drugs by combatants has a long history, recent encounters of professional armed forces have demonstrated the need to reinvestigate the reasons irregular combatants consume drugs, the type of drugs they consume, how they acquire drugs, and the consequences for professional militaries.

0171 **Al-Thagafi, Ahmad, *Causes and Possible Solutions to the Middle East Terrorism,* U.S. Army War College, March 15, 2008. 26pp.**

Terrorism has become a major security issue and world problem. The focus of this research paper will be on the roots of terrorism and the causes of terrorism. It will analyze the causes of terrorism in general and, specifically, the causes of terrorism in the Middle East. One aspect of the Mideast region is the relationship between terrorism and armed struggle to liberate the land. In this regard, the paper will examine how others define terrorism. It will identify possible solutions for dealing with terrorism in the Middle East and show how the return to morality and value may be one of the solutions to eliminate terrorism. It will also analyze how education may provide a solution to preventing the use of terrorism.

0197 **Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism, 2007,* U.S. Department of State, April 2008. 312pp.**

Al-Qa'ida (AQ) and associated networks remained the greatest terrorist threat to the United States and its partners in 2007. It has reconstituted some of its pre-9/11 operational capabilities through the exploitation of Pakistan's Federally Administered Tribal Areas (FATA), replacement of captured or killed operational lieutenants, and the restoration of some central control by its top leadership, in particular Ayman al-Zawahiri. Although Usama bin Ladin remained the group's ideological figurehead, Zawahiri has emerged as AQ's strategic and operational planner. AQ and its affiliates seek to exploit local grievances for their own local and global purposes. They pursue their own goals, often at large personal cost to the local population. These networks are adaptive, quickly evolving new methods in response to countermeasures. AQ utilizes terrorism, as well as subversion, propaganda, and open warfare; it seeks weapons of mass destruction in order to inflict the maximum possible damage on anyone who stands in its way, including other Muslims and/or elders, women, and children. Despite the efforts of both Afghan and Pakistani security forces, instability, coupled with the Islamabad brokered ceasefire agreement in effect for the first half of 2007 along the Pakistan- Afghanistan frontier, appeared to have provided AQ leadership greater mobility and ability to conduct training and operational planning, particularly that targeting Western Europe and the United States. Numerous senior AQ operatives have been captured or killed, but AQ leaders continued to plot attacks and to cultivate stronger operational connections that radiated outward from Pakistan to affiliates throughout the Middle East, North Africa, and Europe.

0509 **Zuhur, Sherifa, *Precision in the Global War on Terror: Inciting Muslims Through the War of Ideas*, Strategic Studies Institute, April 2008. 153pp.**

This monograph questions the messages conveyed to Muslims about their religion and extremism in the war of ideas. Why do American strategic messages on this issue play so badly in the region? Why, despite broad Muslim disapproval of extremism as shown in surveys and official utterances by key Muslim leaders, has support for bin Ladin actually increased in Jordan and in Pakistan since some potting suggests bin Ladin's approval in Jordan suffered a great deal after the hotel bombings? A reason that the United States is winning so few "hearts and minds" in the broader Islamic world is confusion and imprecision in American strategic messages. The grand strategy of defining, isolating, and destroying Islam or radical Islam may not be possible if America does not proceed more carefully, and listen to what its allies think, know, and feel about their faith. This monograph will not revisit the origins of Islamic violence. It is instead concerned with conceptual failure that wrongly constructs the War on Terror and discourages Muslims from supporting it. They are unable to identify with the proposed transformative countermeasures because they discern some of their core beliefs and institutions as targets in this endeavor.

0660 **Shultz, Richard F., *Global Insurgency Strategy and the Salafi Jihad Movement*, Institute for National Security Studies, U.S. Air Force Academy, April 2008. 265pp.**

In this paper, the author differentiates and characterizes terrorists and insurgents, and he conducts a detailed conceptual and historical analysis of insurgency and its current manifestation on a global scale by the Salafi Jihad movement. This work lays out the case that terrorism and insurgency differ, and that the current "long war" is actually being fought by the other side as an insurgency. As a result, the United States must amend and adapt its strategy to one of global counterinsurgency, beyond a global war on terrorism alone.

0924 **National Counterterrorism Center, *2007 Report on Terrorism*, National Counterterrorism Center, April 30, 2008. 96pp.**

Consistent with its statutory mission to serve as the U.S. Government's knowledge bank on international terrorism, the National Counterterrorism Center (NCTC) is providing this report and statistical information to assist in understanding the data. While NCTC keeps statistics on the annual number of incidents of “terrorism,” its ability to track the specific groups responsible for each attack involving killings, kidnappings, and injuries is limited by the availability of reliable open source information, particularly for events involving small numbers of casualties. The statistical material compiled in this report, therefore, is drawn from the number of attacks of “terrorism” that occurred in 2007, which is the closest figure that is practicable for NCTC to supply in satisfaction of the above-referenced statistical requirements. In deriving its figures for terror attacks, NCTC applies the definition of “terrorism” that appears in the 22 U.S.C. 2656f(d)(2), i.e., “premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents.” To establish the repository for the U.S. Government's database on terror attacks, in 2005 NCTC unveiled the Worldwide Incidents Tracking System (WITS). NCTC cautions against placing too much weight on any set of attack data alone to gauge success or failure against the forces of terrorism. Despite limitations, tracking attacks can help the U.S. understand some important trends, including the geographic distribution of incidents and information about the perpetrators and their victims.

REEL 9

Global War on Terrorism cont.

0001 **Zehni, Tevfik, *Turkey and PKK Terrorism*, Naval Postgraduate School, June 2008. 83pp.**

In this thesis, Turkey's struggle against PKK terrorism is analyzed to find an answer to the main research question of this thesis: Why has Turkey not overcome the PKK and its terrorism after thirty years of struggle? To accomplish this, two sub-questions are asked. The first sub-question deals with the perceptions and consequences of terrorism. Consequently, the thesis seeks a comprehensive understanding the motivations of both PKK cadres and Turkish decision makers. The second sub-question seeks to answer the question of why Turkish countermeasures against the PKK's tactics did not put an end to it. Likewise, the second question seeks reasons why PKK terrorism has not achieved the group's political objectives. Hence, the thesis described the mistakes of both parties in the interactive process. The main argument of this thesis is that Turkey has not managed to destroy the PKK because it is entrapped by the PKK's tactics, which aim to make the adversary overreact and force its adversary to implement measures which have counterproductive unintended consequences. Hence, the thesis argues that the PKK has successfully created a gap between the Turkish state and its Turkish citizens with Kurdish origin. Consequently, the PKK has managed to survive for thirty years by convincing these alienated Turkish Kurds to tacitly support the terrorist group.

0084 **Scouras, James, and Jonathan Fox, *Why Have We Not Been Attacked Again? Competing and Complementary Hypotheses for Homeland Attack Frequency*, Advanced Systems and Concepts Office, Defense Threat Reduction Agency, June 2008. 207pp.**

This report is a product of collaborative effort by The Defense Threat Reduction Agency and the Science Applications International Corporation. In this report, the authors present their hypotheses as to why America has not suffered a terrorist attack since the wake of September 11; assess the relative value of improvements to U.S. counterterrorism efforts in response to the attacks of September 11, and to identify implications of newly implemented policy.

0291 **Shannon, William D., *Swarm Tactics and the Doctrinal Void: Lessons from the Chechen Wars*, Naval Postgraduate School, June 2008. 105pp.**

Swarming concepts and swarm tactics have been used for centuries. Swarming is essentially a convergent attack on an adversary from multiple axes. Swarming attacks are usually conducted either by force or fire, or a combination of both. Swarming is not new to military scholars and historians, but the idea of formally incorporating swarming concepts into military doctrine and tactics by the Marine Corps and other U.S. armed forces has never been given serious thought beyond limited experimentation. The most recent and relevant use of swarm tactics occurred during the Chechen Wars against the Russians, which have proved a serious challenge to the Russians. When one examines Marine Corps doctrine, warfighting concepts and experiments, a doctrinal void emerges that should truly be addressed. The Marine Corps distributed operations (DO) concept is reviewed with the idea of contributing toward a future swarming doctrine. While we watched the Chechen Wars unfold, even writing articles and books about all the lessons we should have learned, none of those lessons related to swarming ever translated into real doctrinal changes, embracing both offense and

defense. This thesis asks if there is potential to develop doctrinal swarming concepts, while bringing forth additional lessons learned from the Chechen Wars and highlighting gaps and weaknesses in warfighting doctrinal publications and warfighting experiments.

0397 **McCulloch, Ian, et al., *Change Detection in Social Networks,* U.S. Army Research Institute for the Behavioral and Social Sciences, June 2008. 23pp.**

Social network analysis (SNA) has become an important analytic tool for analyzing terrorist networks, friendly command and control structures, and a wide variety of other applications. This project proposes a new method for detecting change in social networks over time, by applying a cumulative sum statistical process control statistic to normally distributed network measures. The proposed method is able to detect organizational change in the same manner as a quality engineer can detect a change in a manufacturing process. The new algorithm is demonstrated on social network data collected on a group of 24 Army officers going through a 1-year graduate program at Columbia University and on al-Qaeda leading up to and immediately following the terrorist attacks of September 11, 2001.

0423 **Holcombe, Sharon G., and Nathan C. Johnston, *Analysis of the PPBE Process in the Current Dynamic Political Environment,* Naval Postgraduate School, June 2008. 85pp.**

The Planning, Programming and Budgeting (PPB) system was introduced in the Department of Defense (DoD) in the 1960's to link strategies to programs that best satisfy the Nation's policy objectives and fit within budget constraints. Over the past 45 years, modifications were made to the PPB system, and it is now referred to as the Planning, Programming, Budgeting and Execution (PPBE) system, but the original intent of PPB remains intact. Traditionally, wars were funded initially with emergency supplemental funding until the cost of the war could be added into the baseline budget process. The Global War on Terror (GWOT), now in its six year, continues to be funded outside the PPBE process through supplemental appropriations. This project identifies and examines the key factors related to this deviation from the PPBE process. The research analyzes the domestic environment in which PPB was originally implemented and the post 9/11 environment in which it currently exists. A comparative analysis is used to determine the reasons for the increased use of supplementals for baseline and GWOT funding in the last six years. The project also identifies the implications of continued deviation from the PPBE process utilizing parallel budgeting processes.

0507 **Galdorisi, George, et al., *Networking the Global Maritime Partnership,* SPAWAR Systems Center, U.S. Navy, June 2008. 78pp**.

The notion of a “Global Maritime Partnership” is rapidly gaining worldwide currency as many nations and navies seek to work together to combat global terrorism - as well as a host of other issues - in the maritime arena. But neither networking nor global maritime partnerships are new concepts and understanding the history of naval coalition operations and of networking in the maritime environment can help nations and navies understand the challenges to fielding an effective global maritime partnership in the 21st Century. Armed with this historical perspective, coalitions can begin to devise effective solutions to these challenges.

0586 **Massey, Anthony S., *Maritime Security Cooperation in the Strait of Malacca*, Naval Postgraduate School, June 2008. 99pp.**

This thesis examines maritime security cooperation among Singapore, Indonesia, and Malaysia in the Strait of Malacca. Southeast Asian states have traditionally considered multilateral military cooperation among themselves as taboo because of tensions arising from territorial and other political disputes. However, this thesis demonstrates that their aversion to multilateral forms of military cooperation has decreased in the post-9/11 period. This change can be attributed to the relaxation of historical tensions, the recognition of a common threat in piracy and maritime terrorism, an increase in extra-regional pressure to cooperate, and changes in the strategic environment since the end of the Cold War. This thesis also examines the three countries' maritime assets and their procurement strategies to enhance their capabilities to patrol and defend their maritime areas. Although assets are limited, it finds that efforts to coordinate maritime patrols have contributed to a sharp decline since 2004 in attacks on shipping in the Malacca Strait.

0685 **Kimbrough, James M., IV, *Examining U.S. Irregular Warfare Doctrine*, Air Force Institute of Technology, June 2008. 137pp.**

The United States' overwhelming conventional military superiority has forced its enemies for the foreseeable future to fight it unconventionally, mixing modern technology with the classic techniques of insurgency and terrorism. In response to the associated strategic challenges, a growing debate occurred among military historians, strategists, and leaders about the proper principles necessary for contemporary irregular warfare, particularly against a potential transnational enemy. Without a Joint Publication to serve as a guide, several of the individual services have recently published updated doctrine to address the subject: Air Force Doctrine Document (AFDD) 2-3: Irregular Warfare in August in August 2007 and Army Field Manual (FM) 3-24: Counterinsurgency in December 2006 (jointly published as Marine Corps Warfighting Publication 3-33.5: Counterinsurgency). Joint Publication 3-24: Counterinsurgency has an anticipated release of May 2009. The detailed content analysis of AFDD 2-3, FM 3-24, and several authoritative documents required to construct a House of Quality would provide several insights for the doctrine writers; each document would be contrasted against the authoritative works and against each other. Similarities, differences, missing fundamentals, and overarching doctrinal concepts were determined by examining this study's Irregular Warfare Concept House of Quality and can guide the writers in critical concepts for inclusion. Additionally, analysis revealed some implications if the enemy proves to be transitional instead of the more traditional state-base threats.

0821 **Slavin, Barbara, *Mullahs, Money, and Militias*, U.S. Institute of Peace, June 2008. 22pp.**

This report focuses on Iran’s interactions with groups in Lebanon, Iraq, and, to a lesser extent, the Palestinian territories. The intent is to help policymakers understand the real extent of Iranian influence so that they can better motivate Iran and its allies to become more constructive actors in the Middle East.

0843 **Philippone, Douglas, *Hezbollah: The Network and Its Support Systems, Can They Be Stopped?* Naval Postgraduate School, June 2008. 77pp.**

Not all terrorist organizations are rootless groups engaging only in international terrorism. Many terrorist groups are socially intertwined with the local population, highly territorialized, and directly compete for governance. Terrorist groups such as the IRA, Hamas, Mahdi Army, Sendero Luminoso, and Hezbollah are past and present examples of a socially intertwined terrorist organization. These groups present significant, but different challenges to our national security than Al Qaeda does and a different strategy to defeat them may be in order. Using Hezbollah as an example, this thesis addresses the question of whether the direct military approach used to combat terrorist groups, such as Al Qaeda, is appropriate to defeat a socially intertwined terrorist group as well. If not, what techniques would be the most useful?

0920 **General Accountability Office, *Combating Terrorism: Increased Oversight and Accountability Needed Over Pakistan Reimbursement Claims for Coalition Support Funds,* U.S. General Accountability Office, June 2008. 46pp.**

The United States has reimbursed Pakistan, a key ally in the global war on terror, about $5.56 billion in Coalition Support Funds (CSF) for its efforts to combat terrorism along its border with Afghanistan. The Department of Defense (Defense) provides CSF to 27 coalition partners for costs incurred in direct support of U.S. military operations. Pakistan is the largest recipient of CSF, receiving 81 percent of CSF reimbursements as of May 2008. This report focuses on (1) the extent to which Defense has consistently applied its guidance to validate the reimbursements claimed by Pakistan and (2) how the Office of the Defense Representative to Pakistan's (ODRP) role has changed over time. To address these objectives, GAO reviewed CSF oversight procedures, examined CSF documents, and interviewed Defense officials in Washington, D.C., U.S. Central Command in Florida, and Pakistan.

REEL 10

Global War on Terrorism cont.

0001 **Diop Mboup, Moussa, *The African's Perception of the United States' Post- 9/11 Africa Policy and AFRICOM,* U.S. Army Command and General Staff College, June 13, 2008. 184pp.**

The United States' post-9/11 global strategy demonstrates an interest in Africa that contrasts with decades of relative indifference. The 2006 National Security Strategy has stated the United States' commitment to promote security, stability, democracy, and economic prosperity in the continent. Yet, beyond these idealist declarations of good intentions, some foreign policy experts consider that the turnaround in the United States' Africa policy stems from the rising value of the continent for tangible American economic and security interests. They hold the actual objectives of the U.S. to be to secure its access to energy sources, to counter global terrorism, and to contain the influence of China. In that regard, they see the

creation of a dedicated combatant command, the United States Africa Command (AFRICOM), as the reflection of the dramatic evolution in the U.S. policymakers' perceptions of U.S. interests in Africa.' However, the deployment of that unprecedentedly vigorous strategy is facing the reluctance of significant segments of the African intellectual and political elite, due essentially to China's increasing influence, the push-back effect of the War on Terror, AFRICOM's weak security concept, and the continent's marked preference for collective security systems built around its regional organizations and the United Nations.

0185 **General Accountability Office, *Global War on Terrorism: Reported Obligations for the Department of Defense,* U.S. General Accountability Office, June 13, 2008. 11pp.**

Section 1221 of the National Defense Authorization Act for Fiscal Year 2006 requires GAO to submit quarterly updates to Congress on the costs of Operation Iraqi Freedom and Operation Enduring Freedom based on DOD's monthly Supplemental and Cost of War Execution Reports. This report, which responds to this requirement, contains our analysis of DOD's reported obligations for military operations in support of GWOT through September 2008. Specifically, we assessed (1) DOD's cumulative appropriations and reported obligations for military operations in support of GWOT and (2) DOD's fiscal year 2008 reported obligations, the latest data available for GWOT by military service and appropriation account.

0196 **Black, Catherine M., *Legal Implications of the Use of Biometrics as a Tool to Fight the Global War on Terrorism,* U.S. Army Command and General Staff College, June 13, 2008. 86pp.**

Since the fall of the Soviet Union and the emergence of the United States as the world's single superpower, the Army has shifted its threat paradigm from a focus on the Communist threat to that of multiple threats from both nation states and non-state actors. The terrorist attacks against the United States on September 11, 2001, highlighted the need for the country's leadership to develop effective means of identifying personnel as part of a national security plan. National security agents had identified many of the perpetrators of the 9/11 attacks as posing a threat to the United States before the attacks occurred, but they failed to apprehend them in time. If the nation's airports had employed biometric technologies prior to the attacks, it is likely that the Federal Bureau of Investigation (FBI) would have identified and detained the suspects before they were able to carry out their plan. A biometric identification system would present law enforcement officials with a powerful tool for the identification of known or suspected terrorists and other criminals. However, such a system must also adhere to the laws designed to protect the individual privacy of U.S. citizens. System designers would have to ensure that the program adheres to the 4th, 5th, and 14th amendments of the U.S. Constitution as well as the Privacy Act of 1974. Due to the complexity of the topic, it is beyond the scope of this paper to discuss every available biometric technology. The paper will therefore focus on the biometric technologies associated with the Army Battle Command Laboratory's Biometrics Automated Tool Kit (BAT). The BAT allows security personnel to record iris scans, fingerprints, and digital photographs using a portable iris scanner, digital fingerprint collector, and digital camera.

0282 **Newbill, Raymond R., III, *Intelligence Sharing, Fusion Centers, and Homeland Security,* Air Force Institute of Technology, June 19, 2008. 61pp.**

The final report by the bipartisan National Commission on Terrorist Attacks (2004) concluded that the attacks on September 11, 2001 were partly successful because information was not shared properly between agencies. Since that time, the Department of Homeland Security (DHS) and the Department of Defense (DoD) have created a variety of programs and implemented numerous strategies to build a system of information sharing that could detect and prevent large scale physical or cyber terrorist attacks against the critical infrastructures of the United States. The development of "Fusion Centers" across the nation is proving to be an effective intelligence collection, analysis, and dissemination tool for collaboration and information exchange among the private sector, tribal, local, state, and federal authorities as well as the DoD. U.S. Northern Command, the National Guard and DHS are working to improve collaboration via national level exercises such as Cyber Storm I and II. Although legal and privacy concerns exist in balancing the need for National Security with the protection of Civil Liberties, the rise of fusion centers is an indicator that state and local law enforcement as well as public safety agencies have an important role to play in homeland defense and security. As identified in the 9/11 Commission Report, terrorists often live and work in communities during attack planning and may have routine encounters with state and local law enforcement officials prior to an attack. Achieving true Homeland Security may be as simple as first achieving Hometown Security.

0343 **General Accountability Office, *Combating Terrorism: U.S. Oversight of Pakistan Reimbursement Claims for Coalition Support Funds,* U.S. General Accountability Office, June 24, 2008. 20pp.**

The United States has reimbursed Pakistan, a key ally in the global war on terrorism, about $5.56 billion in Coalition Support Funds (CSF) for its efforts to combat terrorism along its border with Afghanistan. The Department of Defense (Defense) provides CSF for costs incurred in direct support of U.S. military operations. Pakistan is the largest recipient of CSF, receiving 81 percent of CSF reimbursements. This testimony focuses on the following: (1) the extent to which Defense has consistently applied its guidance to validate the reimbursements claimed by Pakistan, and (2) how the Office of the Defense Representative to Pakistan's (ODRP) role has changed over time. This statement is based on a concurrently issued GAO report titled "Combating Terrorism: Increased Oversight and Accountability Needed over Pakistan Reimbursement Claims for Coalition Support Funds," GAO-08-806 (Washington, D.C.: June 24, 2008). GAO recommends that Defense consistently implement existing oversight criteria, formalize ODRP's oversight responsibilities, and implement additional controls. Defense generally concurred with the recommendations but stated that the report lacked sufficient context, such as Pakistan's military contributions enabled by CSF and broad legal authority to dispense funds.

0366 **General Accountability Office, *Combating Terrorism: Actions Needed to Enhance Implementation of Trans-Sahara Counterterrorism Partnership,* U.S. General Accountability Office, July 2008. 45pp.**

In 2005 through 2008, the key agencies distributed the majority of the obligated and committed resources to countries in the Sahel region, supporting a range of diplomacy, development assistance, and military activities. In 2005 through 2007, the agencies

distributed about 74 percent of approximately $230 million obligated to the four countries in the Sahel region, about 3 percent to the countries in the Maghreb region, and about 8 percent to the countries in the sub-Saharan region; the remaining 15 percent of the obligations was distributed through regional assistance, such as military exercises in multiple countries. As of June 2008, the agencies expected to distribute about half of approximately $123 million committed for TSCTP for 2008 to the Sahel countries and to distribute the remaining commitments among the Maghreb and Sub-Saharan countries and through regional assistance. The agencies have supported a wide range of activities related to diplomacy, development, and military assistance. For example, State has hosted educational and cultural exchange programs intended to isolate and marginalize violent extremists; USAID supported efforts to improve education and health; and DOD has provided counterterrorism training in marksmanship and border patrol as well as distributed equipment such as vehicles to the militaries of TSCTP partner countries. Several challenges have hampered the key agencies implementation of TSCTP activities, in some cases limiting their ability to collaborate in working to strengthen countries counterterrorism capacity and inhibit the spread of extremist ideology.

0416 **Mihalka, Michael, and David Anderson, *Is the Sky Falling? Energy Security and Transnational Terrorism*, Center for Contemporary Conflict, Naval Postgraduate School, July 2008. 15pp.**

This paper will assess the extent to which transnational terrorists in particular global Jihadists associated with Osama bin Laden have been interested in attacks against the global energy infrastructure.] We then assess the extent to which terrorists have in fact targeted that infrastructure and with what effect. We then place these attacks in the context of other supply disruption events. Finally we make suggestions about a viable way ahead. Western fears about the threat posed by transnational terrorists to energy supplies certainly seem warranted. al-Qaeda has repeatedly threatened to disrupt supplies and have followed up on those threats in a few cases. For example following the attack on the French tanker Limburg in October 2002 al-Qaeda issued a statement that it "was not an incidental strike at a passing tanker but...on the international oil-carrying line in the full sense of the word. Moreover al-Qaeda sees the U.S. intervention in Iraq as strongly linked to the supply of oil.

0431 **Illias, Shayerah, *Islamic Finance: Overview and Policy Concerns*, Congressional Research Service, Library of Congress, July 29, 2008. 7pp.**

Islamic finance is based on principles of "shariah," or "Islamic law." Major principles of shariah are a ban on interest, a ban on uncertainty, adherence to risk-sharing and profit-sharing, promotion of ethical investments that enhance society, and asset-backing. The international market for Islamic finance has grown 10% to 15% annually, in recent years. Islamic finance historically has been concentrated in the Persian Gulf countries, but has expanded globally to both Muslim and non-Muslim countries. There is a small but growing market for Islamic finance in the United States. Through international and domestic regulatory bodies, there has been an effort to standardize regulations in Islamic finance across different countries and financial institutions, although challenges remain. Critics of Islamic finance express concerns about possible ties between Islamic finance and political agendas or terrorist financing and the use of Islamic finance to circumvent U.S. economic

sanctions. Proponents argue that Islamic finance presents significant new business opportunities and provides alternate methods for capital formation and economic development.

0438 **Office of Science and Technology Policy, *Biometrics in Government Post 9/11*, National Science and Technology Council, August 2008. 88pp.**

This report, prepared by the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management, documents key US Government initiatives to advance the science of biometrics and assesses their value in meeting critical operational needs. While federal efforts in biometric technologies predate the terrorist attacks of September 2001 by several decades, this report focuses on progress made since then. Working through the NSTC, and in cooperation with the academic and industrial research communities, agencies embarked on a multi-year initiative to advance the capabilities of biometric technologies. As capabilities advanced, agencies quickly incorporated them into their operational systems and then worked to develop government-wide policies on how to use biometrics to support missions against known and suspected terrorists, while simultaneously enhancing privacy protection for U.S. citizens and foreign visitors. By developing a common planning focus for departments and agencies we have advanced the technology and its operational implementation at a far greater pace than would have been possible otherwise. Today, federal agencies are using biometrics to enhance security and operational efficiency throughout the nation, at the borders and in the battlefields of Afghanistan and Iraq. Their continued efforts to meet the ongoing needs outlined in The National Biometrics Challenge will ensure even greater successes in the future.

0527 **General Accountability Office, *Defense Budget: Independent Review Is Needed to Ensure DOD's Use of Cost Estimating Tool for Contingency Operations Follows Best Practices,* U.S. General Accountability Office, September 2008. 36pp.**

Since the September 2001 terrorist attacks, Congress has provided about $800 billion as of July 2008 to the Department of Defense (DOD) for military operations in support of the Global War on Terrorism (GWOT). GWOT budget requests have grown in scope and the amount requested has increased every year. DOD uses various processes and the Contingency Operations Support Tool (COST) to estimate costs for these operations and to develop budget requests. GAO assessed (1) how DOD uses COST and other processes to develop GWOT budget requests and (2) what actions DOD has taken to ensure COST adheres to best practices for cost estimation. GAO interviewed DOD officials and others to determine how the services develop GWOT budget requests using COST and other processes. GAO also used its Cost Assessment Guide as criteria for best practices for cost estimation. GAO is recommending that DOD (1) arrange for an independent review of COST to ensure that the model adheres to best practices and (2) consider options for refining COST to better meet the needs of the services. DOD agreed with both of GAO's recommendations.

0568 **Pena-Guzman, Claudia P., *Exploitation of Free Markets and Globalization to Finance Terrorists*, Naval Postgraduate School, September 2008. 69pp.**

The international community has taken measures to monitor financial networks through anti-money laundering acts, which since 9/11 have expanded to cover terrorist financing. However, the strides made to date in some parts of the world have been limited and gaps still

exist that terrorist organizations can infiltrate to thwart the international community's efforts. The purpose of this study is to provide an overview of current international counter-terrorist financing efforts and how terrorists exploit them. The project consisted of three case studies. Colombia is the primary case, while Peru and Great Britain are secondary cases. Through these case studies, the author identifies how terrorist organizations are taking advantage of systems of financial globalization and free markets in these countries to finance their activities. The four elements studied in each country are its economy, financial markets and banking system, auditing and internal monitoring system, and international cooperation to combat terrorist financing. In Colombia, the study focuses on the Revolutionary Armed Forces of Colombia (FARC), the National Liberation Army (ELN), and the United Self-Defense Forces of Colombia (AUC), and how the Colombian government and financial institutions have responded to them. In Peru, the focus of the examination is Sendero Luminoso, and in Great Britain, it is the Irish Republican Army in Northern Ireland.

0637 **General Accountability Office,** ***Military Operations: DOD Needs to Address Contract Oversight and Quality Assurance Issues for Contracts Used to Support Contingency Operations,*** **U.S. General Accountability Office, September 2008. 47pp.**

The Department of Defense (DOD) uses contractors to meet many of its logistical and operational support needs. With the global war on terrorism, there has been a significant increase in deployment of contractor personnel to areas such as Iraq and Afghanistan. In its fiscal year 2007 report, the House Appropriations Committee directed GAO to examine the link between the growth in DOD's operation and maintenance costs and DOD's increased reliance on service contracts. GAO determined (1) the extent to which costs for selected contracts increased and the factors causing the increases, (2) the extent to which DOD provided oversight for selected contracts, and (3) the reasons for DOD's use of contractors to support contingency operations. To address these objectives, GAO reviewed a non-probability sample of seven DOD contracts for services that provide vital support to contingency operations in Iraq and Afghanistan. GAO reviewed contract requirements, funding documents and DOD guidance for these contracts and interviewed DOD and contractor personnel. To ensure effective oversight, GAO recommends that DOD adequately staff oversight positions with qualified personnel, and address inconsistencies in maintaining contract files and implementing quality assurance principles. DOD concurred with each of GAO's recommendations and stated the Army was aware of and addressing the identified problems.

0685 **Maples, L. D. M.,** ***Terrorism 101: Knowledge About the "What and Why" of Terrorism as a State and Local Law Enforcement Competency,*** **Naval Postgraduate School, September 2008. 95pp.**

In the wake of the September 11, 2001, terrorist attacks, state and local police agencies were thrust into new homeland security related roles. One area specifically identified in national strategies and, then, supported by expert opinions for enhancing law enforcement's abilities to prevent terrorism is through enhanced knowledge and education regarding terrorism. Terrorism has been the subject of academic work even prior to the 9/11 attacks. Some of this work has looked at the underlying causes that compel people to threaten and use violence to achieve their individual or group objectives. This body of work is a resource for law enforcement to bridge gaps between national strategies and current practices. The primary focus of this research is to assess the current state of terrorism training for state and local law

enforcement officials. It looks at whether the subject of terrorism is a core professional competency for law enforcement officials in every state and, specifically, if state and local police are being exposed to knowledge about the causes and motivations associated with terrorism in order to better understand, and ultimately, prevent it. Surveys and interviews of state officials are conducted in order to gather data about the current state of terrorism related training throughout the nation. A qualitative analysis is conducted in order to further assess the content of select course content and identify potential training and educational gaps.

0780 **Department of Homeland Security*, One Team, One Mission, Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan, Fiscal Years 2008-2013*, Department of Homeland Security, September 2008. 44pp.**

This Department of Homeland Security's overriding and urgent mission is to lead the unified national effort to secure the country and preserve our freedoms. While the Department was created to secure our country against those who seek to disrupt the American way of life, our charter also includes preparation for and response to all hazards and disasters. The citizens of the United States must have the utmost confidence that the Department can execute both of these missions. The 2008 Strategic Plan serves to focus the Department's mission and sharpen operational effectiveness, particularly in delivering services in support of Department-wide initiatives and the other mission goals. It identifies the goals and objectives by which we continually assess our performance. The Department uses performance measures at all levels to monitor our strategic progress and program success. This process also keeps the Department's priorities aligned, linking programs and operations to performance measures, mission goals, resource priorities, and strategic objectives.

0822 **Biddle, Stephen, *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy*, Strategic Studies Institute, September 2008. 110pp.**

Hezbollah's conduct of its 2006 campaign in southern Lebanon has become an increasingly important case for the U.S. defense debate. Some see the future of warfare as one of non-state opponents employing irregular methods, and advocate a sweeping transformation of the U.S. military to meet such threats. Others point to the 2006 campaign as an example of a non-state actor nevertheless waging a state like conventional war, and argue that a more traditional U.S. military posture is needed to deal with such enemies in the future. This monograph, by Dr. Stephen Biddle of the Council on Foreign Relations and Mr. Jeffrey Friedman, Harvard Kennedy School of Government, seeks to inform this debate by examining in detail Hezbollah's conduct of the 2006 campaign. The authors use evidence collected from a series of 36 primary source interviews with Israeli participants in the fighting who were in a position to observe Hezbollah's actual behavior in the fiend in 2006, coupled with deductive inference from observable Hezbollah behavior in the field to findings for their target strategic intent for the campaign.

0933 **Chau, Donovan C., *U.S. Counterterrorism in Sub-Saharan Africa: Understanding Costs, Cultures, and Conflicts*, Strategic Studies Institute, September 2008. 81pp.**

While sub-Saharan Africa (SSA) has never been the centerpiece of U.S. foreign or defense policy, the current struggle of the United States and its allies against terrorist groups and individuals motivated by Islamic extremism has elevated the region to a front in the global conflict. In this Letort Paper, Dr. Donovan C. Chau examines U.S. counterterrorism policy in

SSA. He begins by analyzing the policy debate in Washington, DC, especially the fundamental divergence of approaches between development and defense. From there, the paper shifts to a discussion of the attitudes and views of terrorism and counterterrorism in SSA. Vast and diverse, SSA is divided subregionally into East, West, and Southern Africa so as to highlight the different geographies, histories, threats, and perceptions. Given the debate in Washington and the perspectives from SSA, Dr. Chau answers the central question concerning the most effective long-term approach to counterterrorism in SSA. He suggests a grand strategic approach to attain "three standards" that comprise seizing and holding the moral high ground, winning the struggle for perceived legitimacy, and pursuing restrained counterterrorism responses.

REEL 11

Global War on Terrorism cont.

0001 **Addicott, Jeffrey, *Congressionally-Direct Homeland Defense and Civil Support Threat Information Collection,* St. Mary's University of San Antonio and U.S. Air Force Research Laboratory, September 2008. 31pp.**

The objective of this effort was to collect and analyze all applicable non-release statutory provisions associated with the "open government" laws of all 50 states since September 11, 2001, in order to create a full understanding that will not only inform the public as to the actions of the states in this regard but also to assist federal, state, and local government employees, to include policy makers, in better safeguarding critical infrastructure and information systems while complying with security policies that assure the fullest level of public access to information. In addition, the comprehensive study included a first ever compilation of the non-release provisions from four nations facing serious terrorism threats -- Israel, Colombia, France, and the United Kingdom. The primary byproducts of the study consisted of two published books. Entitled: "State Open Government Law and Practice in a Post-9/11 World," the first and most significant of the two books is a complete state-by-state guide containing all non-release statutes of the 50 states as well as selected changes in national public information laws in Colombia, France, Israel, and the United Kingdom. The second book, "Selected Essays on State Open Government Law and Practice in a Post-9/11 World (2008)," details the opinions from leading subject matter experts on the information provided in the first book. All aspects of the study are available to public access in printed or electronic formats.

0032 **Tiwari, Andre, *Small Boat and Swarm Defense: A Gap Study,* Naval Postgraduate School, September 2008. 87pp.**

United States Naval forces conducting straits transits face a host of unique force protection challenges. Traffic density is often high, with many ferries, fishing and pleasure boats, and large cargo ships maneuvering in a small area. Although the Rules of Engagement (ROE) will generally designate query and warning ranges, International law and freedom of navigation allow vessels to operate in very close proximity to warships. Small vessels are often difficult to regulate and many lack basic equipment such as bridge to bridge radios. With a host of stationary and seemingly randomly moving boats, determining a hostile action

in a timely manner is difficult at best. These conditions make the identification of and defense against hostile small craft extremely difficult. Even after a craft is designated hostile, the timeline for mounting an effective defense is often very short. This thesis shows that a gap in capability exists in the surface force to defend itself against small threat craft. It adds functionality to the Anti-Terrorism / Force Protection (AT/FP) Tool initially developed by Lieutenant James Harney and significantly enhanced by Lieutenant Patrick Sullivan. Lieutenant Harney created the foundation for all the work that followed by investigating the role of Discrete Event Simulation (DES) in defense Modeling and Simulation (M&S). The result of this work was a fully integrated, prototypical, Java-based application that demonstrates how various Open-Source, web-based technologies can be applied in order to provide the tactical operator with tools to aid in Force Protection planning.

0118 **Burchnell, Ryan,** ***Dynamic Personal Identity and the Dynamic Identity Grid: How Theory and Concept Can Transform Information Into Knowledge and Secure the American Homeland,*** **Naval Postgraduate School, September 2008. 130pp.**

Personal identification systems and processes; including those used for transliteration, travel visas and driver licenses; have failed to adequately adapt to the nation's new asymmetric threat. After September 11th, personal identification information about the attackers began to emerge and it became clear that it could have been used to identify the attackers prior to their terrorist acts. This study used qualitative research methods to construct meaning from previously uncorrelated issues and employed a three stage analytical approach that grounded the research. The tertiary stage identified themes that had theoretical relevance and, in turn, a direct impact on the proposed solutions. The study borrowed concepts from a handful of formal qualitative methods; including grounded theory, content/document analysis, interviewing, triangulation and conceptual modeling. It found that ambiguity and ethnocentricity is inherent in American name-based identity collection practices, systems and processes; that consistently collecting specific name-based characteristics could be highly beneficial to combating terrorism; and that by leveraging the knowledge created by consistent collection practices, systems and processes we can transform name-based identity into a dynamic and leverage-able commodity. To effectively do so, this project presents a substantive theory, Dynamic Personal Identity, and a conceptual technological system, the Dynamic Identity Grid, as potential solutions.

0247 **Ludwick, Keith W.,** ***Closing the Gap: Measuring the Social Identity of Terrorists,*** **Naval Postgraduate School, September 2008. 79pp.**

Studies of terrorism today focus on psychological and behavioral aspects of individuals. Most research shows that using a single model in an attempt to profile terrorists psychologically is problematic, if not impossible. However, using two well-established theories from social psychology, Social Identity Theory and Social Distance Theory, allows the development of a practical model to develop a social profile of a terrorist group. From that, it is further possible to use the resulting social profile to compare terrorist groups against each other in order to develop predictive models as to the propensity of violence of a particular group. To test this, the research within this thesis uses open source interviews of the terrorist group HAMAS and the Popular Front for the Liberation of Palestine (PFLP), taken from on-line magazines, on-line journals, on-line newspapers, and official web sites, to serve as respondents to a survey instrument developed from other social identity studies. The results of this research shows that a social profile of a terrorist group can be developed from

standard social identity measurement survey instruments, and it is possible to develop practical methods for comparing groups, based on their social identities, to predict their propensity to violence.

0325 **Migdalovitz, Carol, *Israeli-Arab Negotiations: Background, Conflicts, and U.S. Policy*, Congressional Research Service, Library of Congress, September 8, 2008. 46pp.**

After the first Gulf war, in 1991, a new peace process consisting of bilateral negotiations between Israel and the Palestinians, Jordan, Syria, and Lebanon achieved mixed results. The post 9/11 war on terrorism prompted renewed U.S. focus on a peace process, emphasizing as its goal a democratic Palestinian state as a precondition for achieving peace. On April 30, 2003, the United States, the U.N., European Union, and Russia (known as the "Quartet") presented a "Roadmap" to Palestinian statehood. Neither Israel nor the Palestinians have implemented it. Israel unilaterally disengaged (withdrew) from the Gaza Strip and four small settlements in the West Bank in August 2005. Chairman/President Yasir Arafat died on November 11, 2004; on January 9, 2005, Mahmud Abbas was elected to succeed him and he seeks final status talks. The victory of Hamas, which Israel and the United States consider a terrorist group, in the January 2006 Palestinian parliamentary elections, however, complicated the situation. The United States, Israel, and the Quartet agreed that they will not deal with a Hamas-led government until it disavows violence, recognizes Israel, and accepts prior Israeli-Palestinian accords. The rise of Hamas and the conflicts in Gaza and Lebanon sparked by the Hamas and Hezbollah kidnappings of Israeli soldiers cast shadows on the prospects for future talks.

0372 **O'Rourke, Ronald, *Navy Role in Global War on Terrorism (GWOT)—Background and Issues for Congress*, Congressional Research Service, Library of Congress, September 11, 2008. 7pp.**

The Navy is taking several actions to expand its capabilities for participating in the Global War on Terrorism (GWOT). The Navy's role in the GWOT raises several potential oversight issues for Congress, including the need for an increased Navy role, and the amount of Navy personnel and funding associated with GWOT-related activities.

0379 **General Accountability Office, *Global War on Terrorism: Reported Obligations for the Department of Defense,* U.S. General Accountability Office, September 15, 2008. 12pp.**

This report contains the GAO's analysis of DOD's obligations for military operations in support of GWOT through June 2008. Specifically, they assessed DOD's cumulative appropriations and reported obligations for military operations in support of GWOT, and DOD's fiscal year 2008 reported obligations from October 2007 through June 2008, the latest data available for GWOT by military service and appropriation account. As of September 2008, Congress has appropriated a total of about $807 billion primarily for GWOT operations since 2001. Of that amount, about $187 billion has been provided for fiscal year 2008 and about $65.9 billion has been appropriated for use in fiscal year 2009.

0391 **Browder, Dewey A., and Greg Kaufmann, *Stability Operations and State-Building: Continuities and Contingencies,* Strategic Studies Institute, October 2008, 280pp.**

The purpose of this academic colloquium was to identify principles and supporting policies of state-building that will enhance America's ability "to win the peace" while stabilizing chaotic regions. Basic to the concept of the colloquium was the idea that just as there are acknowledged principles of war that enhance the possibility of victory on the battlefield, there should be principles that, if applied during the state-building process, will enhance the chances of "winning the peace." The idea that principles should constitute the foundation of state-building and that supporting policies and procedures then flow from those principles was fundamental to the colloquium's process. The participants included scholars from a wide range of academic disciplines, active duty military personnel, nongovernmental organization staff, and governmental administrators. The colloquium's sponsors endeavored to blend the expertise of civilian academics and military professionals. After all scheduled presentations, six independent breakout groups distilled the consolidated list of principles to a common core for each group. Next, a plenary session considered the resulting six lists of principles for further consolidation into a core list of six principles. Those principles are as follows: (1) rule of law, (2) security (military, economic, and civil), (3) legitimacy, (4) development (the encouragement thereof), (5) self-empowerment/self-sufficiency, and (6) communications (intergovernmental and international).

0672 **Felter, Joseph, and Brian Fishman, *Iranian Strategy in Iraq: Politics and "Other Means",* Combating Terrorism Center, U.S. Military Academy, October 13, 2008. 90pp.**

Iran has a robust program to exert influence in Iraq to limit American power projection capability in the Middle East, ensure the Iraqi government does not pose a threat to Iran, and build a reliable platform for projecting influence further abroad. Iran has two primary modes of influence. First, and most importantly, it projects political influence by leveraging close historical relationships with several Shi'a organizations in Iraq: the Islamic Supreme Council of Iraq (ISCI), the Badr organization, and the Dawah political party. Second, Iran uses the Iranian Revolutionary Guard Corps (IRGC) and Qods Force (QF) to provide aid in the form of paramilitary training, weapons, and equipment to various Iraqi militant groups, including Moqtada al-Sadr's Jaysh al-Mahdi (JAM) and the Special Group Criminals (SGCs). Iranian influence in Iraq is inevitable, and some of it is legal and constructive. Nonetheless, Iranian policy in Iraq is also duplicitous. Iran publicly calls for stability while subverting Iraq's government and illegally sponsoring anti-government militias. Iran has achieved three major accomplishments in Iraq. First, the unstable security situation and political opposition means the United States is not in a position to use Iraq as a platform for targeting Iran. Second, Iran's political allies have secured high-ranking positions in the Iraqi government. Third, the Iraqi constitution calls for a highly federalized state. Iran values a decentralized Iraq because it will be less capable of projecting power, and because Iran is primarily concerned with Iraq's southern, oil rich, Shi'a dominated provinces. In addition to public sources, this report draws on a substantial body of information never before released to the public. These include internal Iraqi intelligence documents written before 2003, details from reports of Significant Activities by U.S. and Coalition Forces, as well as summaries of interrogations of detained militants.

0763 **Doughtery, Edmond J.,** ***Scalable Emergency Response System for Oceangoing Assets, Report on Top Level Designs,*** **Ablaze Development Corporation and Office of Naval Research, October 20, 2008. 205pp.**

The scalable emergency system is intended to cover the full scale of possible at-sea incidents from the routine to the rare; from the detection and decontamination of a single piece of equipment before it is loaded on a vessel, to the response, rescue, containment and rehabilitation of a vessel in open waters. The system will be able to safely and quickly decontaminate cargo and personnel, as well as entire vessels at sea and in port. This report finalizes the top level design of the four (4) primary concepts selected for the program.

0967 **Freier, Nathan,** ***Known Unknowns: Unconventional "Strategic Shocks" in Defense Strategy Development,*** **Strategic Studies Institute, November 2008. 51pp.**

The current defense team confronted a game-changing "strategic shock" in its first 8 months in office. The next team would be well-advised to expect the same. Defense-relevant strategic shocks jolt convention to such an extent that they force sudden, unanticipated change in the Department of Defense's (DoD) perceptions about threat, vulnerability, and strategic response. Their unanticipated onset forces the entire defense enterprise to reorient and restructure and confront challenges fundamentally different than those routinely considered in defense calculations. The likeliest and most dangerous future shocks will be unconventional. They will manifest themselves in ways far outside established defense convention. Most will be nonmilitary, and not defense-specific events conducive to the conventional employment of the DoD enterprise. Their origin is most likely to be in irregular, catastrophic, and hybrid threats of purpose (emerging from hostile design) or threats of context (emerging in the absence of hostile purpose or design). Thoughtful evaluation of defense-relevant strategic shocks and their deliberate integration into DoD strategy and planning is a key check against excessive convention.

REEL 12

Global War on Terrorism cont.

0001 **Subcommittee on Domestic Improvised Explosive Devices,** ***Research Challenges in Combating Terrorist Use of Explosives in the United States,*** **National Science and Technology, December 2008. 47pp**.

Terrorists have repeatedly shown their willingness and ability to use explosives as weapons worldwide and there is ample evidence to support the conclusion that they will continue to use such devices to inflict harm. In acknowledgement of this threat, the President issued Homeland Security Presidential Directive 19 (HSPD-19), *Combating Terrorist Use of Explosives in the United States*, which establishes overall national policy, and calls for the development of a national strategy and an implementation plan to deter, prevent, detect, protect against, and respond to terrorist use of explosives in the United States. The Department of Justice (DOJ) and the Department of Homeland Security (DHS), in coordination with the Department of Defense (DoD) and other interagency partners, developed the National Strategy to Combat Terrorist Use of Explosives in the United States

and the HSPD-19 Implementation Plan, which provide a way forward. Both the National Strategy and the Implementation Plan highlight the importance of a coordinated approach to a counter-IED (C-IED) RDT&E program. The co-chairs of the NSTC CHNS, with concurrence from the Office of Science and Technology Policy (OSTP) and the Homeland Security Council (HSC), established the Subcommittee on Domestic IEDs (D-IED SC) to serve as the formal mechanism for this coordination. The membership of the D-IED SC comprises representatives of the organizations in the Federal government that have responsibilities in the area of countering the terrorist use of IEDs.

0048 **Kronstadt, K. Alan, *Terrorist Attacks in Mumbai, India, and Implications for U.S. Interests*, Congressional Research Service, Library of Congress. 22pp.**

On the evening of November 26, 2008, a number of well-trained militants came ashore from the Arabian Sea on small boats and attacked numerous high-profile targets in Mumbai, India, with automatic weapons and explosives. By the time the episode ended some 62 hours later, about 165 people, along with nine terrorists, had been killed and hundreds more injured. Among the multiple sites attacked in the peninsular city known as India's business and entertainment capital were two luxury hotels -- the Taj Mahal Palace and the Oberoi-Trident -- along with the main railway terminal, a Jewish cultural center, a cafe frequented by foreigners, a cinema house, and two hospitals. Six American citizens were among the 26 foreigners reported dead. Indian officials have concluded that the attackers numbered only 10, one of whom was captured. The investigation into the attacks is still in preliminary stages, but press reporting and statements from U.S. and Indian authorities strongly suggest that the attackers came to India from neighboring Pakistan and that the perpetrators likely were members and acting under the orchestration of the Pakistan-based Lashkar-e-Taiba (LeT) terrorist group. The LeT is believed to have past links with Pakistan's military and intelligence services. By some accounts, these links are ongoing, leading to suspicions, but no known evidence, of involvement in the attack by Pakistani state elements. The Islamabad government has strongly condemned the Mumbai terrorism and offered New Delhi its full cooperation with the ongoing investigation, but mutual acrimony clouds such an effort, and the attacks have brought into question the viability of a nearly 5-year-old bilateral peace process between India and Pakistan. The Mumbai attacks have brought even more intense international attention to the increasingly deadly and destabilizing incidence of Islamist extremism in South Asia, and they may affect the course of U.S. policy toward Pakistan.

Al-Qaeda

0070 **Brachman, Jarret M., and William F. McCants, *Stealing Al-Qa'ida's Playbook*, Combating Terrorism Center, U.S. Military Academy, February 2006. 25pp.**

The key to defeating the jihadi movement is identifying its strengths and weaknesses so that the former may be countered or co-opted and the latter exploited. In this article we argue that the people who know these strengths and weaknesses best are the jihadis themselves; one just needs to know where (and how) to look for their insights. Jihadi leaders are surprisingly frank when discussing the vulnerabilities of their movement and their strategies for toppling local regimes and undermining the United States. Their candor is, in large part, a consequence of struggles for leadership within the movement; thus, a leader of one group

will publish his strategic vision in order to gain more recruits and achieve a reputation as a serious scholar worthy of respect. It is also a consequence of the United States success in destroying jihadi training camps and denying safe havens jihadi leaders have had to put their writings online so as to provide continuing guidance to a very decentralized following. In a sense, members of the jihadi movement have put their team's playbooks online. By mining these texts for their tactical and strategic insights, the United States will be able to craft effective tactics, techniques, and procedures to defeat followers of the movement. In what follows, we will demonstrate the efficacy of this approach by highlighting the insights we have gleaned from the works of four prominent jihadi ideologues.

0095 **Combating Terrorism Center, *Harmony and Disharmony: Exploiting al-Qa'ida's Organizational Vulnerabilities*, Combating Terrorism Center, U.S. Military Academy, February 14, 2006. 115pp**.

In war, traditional nation-states have specific attributes, such as territory, military forces, governmental structures, and economic capacity that can be the objectives of grand strategy and resulting military campaigns. Non-state actors, such as al-Qa'ida, do not have these same centers of gravity. Al-Qa'ida has non-traditional strengths and weaknesses reflecting its own unique human personalities, structure, organization, processes, and procedures. The purpose of this study is to examine the internal characteristics of al-Qa'ida so that policymakers and analysts can develop strategies to focus on their key vulnerabilities and degrade their effectiveness in supporting the global Salafist insurgency. One of the best ways to learn about al-Qa'ida is to read the papers, manuals, and other documents which al-Qa'ida leaders have written to guide and discipline their own enterprise. Many of these documents have been captured by military and law enforcement forces and can provide insight into the way the organization works. Other key references are readily available on the World Wide Web. The Combating Terrorism Center (CTC) at West Point was given 28 recently de-classified documents from the Defense Department's "Harmony" database, which consists of literally thousands of documents. Analyzing these documents is akin to gathering several parts of a complex jigsaw puzzle. The documents themselves are interesting, but to get a more complete picture, the CTC authors found that it was important to combine the pieces from the al-Qa'ida documents, other published reports, books, articles, and studies on al-Qa'ida, organization theory, and other similar historical cases. The resulting analysis attempts to provide a complex but coherent assessment of al-Qa'ida's organization, identifying several areas of vulnerability and potential strategies to exploit these vulnerabilities.

0210 **Hazdra, Richard J., *Al Qaeda as a System*, U.S. Army War College, March 15, 2006. 23pp.**

With the correct military strategy, the US military can provide the main effort to win the Global War on Terrorism (GWOT) and Col Warden's five-ring model is useful to determine target sets for that effort. Col Warden developed the five-ring model to analyze the sources of power of an enemy and target those sources of power for disruption or destruction. It is necessary to briefly review Col Warden's five-ring theory that looks at leadership, organic essentials, infrastructure, population, and fielded forces as five parts of a system. Although some strategists believe that the five-ring model is applicable only to nation-states, Col Warden suggested it is applicable to non-state organizations such as a terrorist organization even though the target sets and the instruments of national power to affect those target sets may be different than those of a nation-state. Also, some believe that Col Warden's five-ring

theory applies to only aerial bombing. It does not, as this paper will demonstrate. A terrorist organization can be analyzed as a system, because to wage violence, a terrorist organization still requires sources of power and logistics. Al Qaeda serves as the example used in analyzing a terrorist organization in the model. In addition, it is important to identify and understand terrorist objectives and terrorist motivations to achieve their goals. This paper is analysis of Al Qaeda as a system and identifies Al Qaeda's subsystems.

0233 **Naji, Abu Bakr (Translated by William McCants),** ***The Management of Savagery: The Most Critical Stage Through Which the Umma Will Pass,*** **John M. Olin Institute for Strategic Studies, Harvard University, May 23, 2006. 268pp**.

Management of Savagery is an open and frank description of the need to create and manage nationalist and religious resentment and violence in order to create long-term propaganda opportunities for jihadist groups. Most notably, the author discusses the value of provoking military responses by superpowers in order to recruit and train guerilla fighters and to create martyrs. Naji suggests that a long-lasting strategy of attrition will reveal fundamental weaknesses in the abilities of superpowers to defeat committed Jihadists. Naji uses the philosophy of Ibn Taymiyya, the influential 14th century theologian, and his book also displays a thoughtful understanding of western institutions and value systems, and the role and history of Islamist movements in Egypt, Afghanistan, and the Middle East, particularly the activities of Islamic Jihad in Egypt during the 1990s. This book was authored by Abu Bakr Naji who is unidentified, and is known only for this piece plus some contributions to the al-Qaeda online magazine Sawt al-Jihad. Some believe Naji's book has influenced al-Qaeda.

0501 **House Permanent Select Committee on Intelligence,** ***Al-Qaeda: The Many Faces of an Islamist Extremist Threat,*** **House Permanent Select Committee on Intelligence, June 2006. 45pp.**

Nine years after the September 11, 2001 terrorist attacks, the United States remains a nation at war. Al-Qaeda and Islamist extremist terrorist groups with like-minded goals and ideologies remain one of the most immediate strategic threats to the national security of the United States. Nonetheless, the threat faced today is quite different from the terrorist threat that was faced prior to September 11, 2001. The United States has taken positive steps to enhance our national security against the threat of future terrorist attacks. However, the threat of terrorism is still very real, and in many ways more alarming than the threat that existed prior to September 11, 2001. There are a growing number of groups building the capability to attack the United States, our allies, and our interests abroad. The United States must remain vigilant in the face of these threats and provide our intelligence, law enforcement and military personnel the necessary legal authorities, resources and tools to protect our national security.

0546 **Ackerman, Gary,** ***The Jericho Option: Al-Qa'ida and Attacks on Critical Infrastructure,*** **Lawrence Livermore National Library, June 8, 2006. 320pp.**

There is no doubt that al-Qaida and its affiliates have displayed, and continue to display, an acute interest in attacking targets that are considered to be important components of the infrastructure of the United States. What has not thus far been carried out, however, is an in-depth examination of the basic nature, historical evolution, and present scope of the

organization's objectives that might help government personnel develop sound policy recommendations and analytical indicators to assist in detecting and interdicting plots of this nature. This study was completed with the financial support of the Lawrence Livermore National Laboratory, through a project sponsored by the U.S. Department of Homeland Security, Science and Technology Directorate. It is specifically intended to increase counterterrorism analysts understanding of certain features of al-Qaida's strategy and operations in order to facilitate the anticipation and prevention of attacks directed against our most critical infrastructures.

0868 **O'Quinn, Charles R. V., *An Invisible Scalpel: Low-Visibility Operations in the War on Terrorism*, U.S. Army Command and General Staff College, June 16, 2006. 100pp.**

The War on Terror (WOT) is actually a war against extremist insurgents comprised of numerous and varied organizations scattered across the globe. They are spurred to action by an extremist ideology that is nurtured, demonstrated, and led by al Qaeda and its leadership. This ideology serves as the insurgency's center of gravity whereby it gains all manner of support across a broad spectrum of functional resources in multiple operational domains. As operating environments change, these ideology-inspired decentralized insurgent organizations are able to quickly adapt their methods of operation. In order to defeat this evolving, ubiquitous yet elusive threat, the US must develop a comprehensive strategy that incorporates all instruments of US national power, as well as those of its allies. This strategy must also defeat or mitigate the enemy's center of gravity in order to have any chance of success. This thesis argues that as lead combatant command in the WOT, the US Special Operations Command (USSOCOM) should conduct continuous, global, preemptive low-visibility operations in order to disrupt insurgent operations. In order to accomplish its WOT missions, USSOCOM must effectively organize and array forces and resources to defeat insurgent functional resources across multiple operational domains.

0968 **Witty, David M., *Attacking Al-Qaeda's Operational Centers of Gravity*, U.S. Naval War College, October 23, 2006. 31pp.**

The doctrinal basis for defeating an enemy is the proper identification of an enemy's center of gravity (COG) and attacking it. This concept is applicable to the War on Terror. Al-Qaeda is an ideology and an organization providing operational level inspiration and guidance to insurgencies throughout the Muslim world. Al-Qaeda's basis of support among Muslims is its ideology - a rejection of the West and return to fundamentalist Islam. This ideology is al-Qaeda's strategic COG. Al-Qaeda's struggle is best understood as a global insurgency with many local insurgency subsets rather than a global war of terror. Each local insurgency is connected to al-Qaeda's global insurgent war against the West through ideology. At the operational level, an insurgency's COG is the population's support, and this is al- Qaeda's operational COG. Al-Qaeda's ideology attracts the population and local insurgents to al-Qaeda, which in turn connects theater of operations insurgencies to al-Qaeda's global war. By attacking the al-Qaeda ideology at the operational level, an operational commander can weaken an insurgency by making it a local affair not connected to the larger global struggle. The al-Qaeda ideology is a decisive point at the operational level of counterinsurgency.

0999 **Nagma, Elmer, *Disarming the Bearer of the Sword: Delinking the Abu Sayyaf from the Global Insurgency*, U.S. Naval War College, October 23, 2006. 23pp.**

On May 27, 2001, the Abu Sayyaf Group (ASG), an Al Qaeda affiliate, gained worldwide notoriety when it attacked a popular vacation resort on the Philippine island of Palawan. Thirty tourists were kidnapped for ransom. One of the vacationers, Guillermo Sobero, was an American from Corona, California. Weeks after the kidnapping the ASG announced it had beheaded Sobero. Also abducted was an American missionary couple, Martin and Gracia Burnham of Wichita, Kansas. After a year in captivity in the dense, mountainous jungles of Mindanao, an injured Gracia Burnham was rescued by the Armed Forces of the Philippines (AFP). Tragically, her husband was killed during the fierce skirmish of the rescue attempt.

1022 **Fishman, Brian, *Al-Qa'ida's Spymaster Analyzes the U.S. Intelligence Community*, Combating Terrorism Center, U.S. Military Academy, November 6, 2006. 6pp.**

On August 6, 2006 Al Jazeera broadcast a video in which Ayman al-Zawahiri claimed that al-Gamaa al-Islamiya (Egyptian Islamic Group—Gamaa Islamiya)) had joined Al-Qa'ida. The video also included Muhammad Khalil al-Hakaymah—a player in Egyptian Islamist movements since 1979—swearing allegiance to Al-Qa'ida on behalf of the Egyptian group. Despite al-Zawahiri's star power, al-Hakaymah's claims were subsequently disputed by members of al-Gamaa al-Islamiya, which had formally renounced violence in 1997. Al-Hakaymah's bayat to Al-Qa'ida corresponded with the publication of his book, *The Myth of Delusion*, a detailed dissertation designed to de-mystify the U.S. intelligence community. Arab observers, in and outside of Egypt, have since speculated that Al-Hakaymah will play an increasingly significant role in Al-Qa'ida because of his expertise on the United States security community and disillusionment with Gamaa Islamiya's non-violent approach.

REEL 13

Al-Qaeda cont.

0001 **Browne, William W., III*Constituency Constraints on Violence: Al-Qaeda and WMD*, Naval Postgraduate School, December 2006. 88pp.**

The changing nature of terrorist attacks in the previous decade has cast doubt on the commonly accepted constraints on terrorist violence. Claims that these constraints are eroding has led to an unstudied assumption that modern terrorist groups, and al-Qaeda in particular, are not subject to constituency constraints. Most alarming is the possibility that al-Qaeda, allegedly unconcerned with alienating supporters, will attack the United States with weapons of mass destruction (WMD). Yet no detailed study of al-Qaeda's constituency constraints has been undertaken, even though they devote considerable effort to win popular support among Muslims. This thesis reveals that al-Qaeda seeks the support of a constituency as the central pillar of their strategy. This constituency, contrary to Western portrayals, largely does not support indiscriminate killing and would not support a WMD attack. Al-Qaeda is aware of this sentiment, and as a pragmatic group is willing to alter their methods to gain supporters. Consequently, al-Qaeda is not likely to conduct such an attack for fear of alienating this constituency.

0089 **Rabassa, Angel, et al.,** ***Beyond al-Qaeda, Part 1: The Global Jihadist Movement,*** **Project Air Force, December 2006. 228pp.**

Defeating the global jihadist movement--which is defined as al-Qaeda and the universe of jihadist groups that are associated with or inspired by al-Qaeda--is the most pressing security challenge facing the United States. The global jihadist movement can be distinguished from traditional or local jihads, which are armed campaigns conducted by Islamist groups against local adversaries with usually limited aims and geographic scope, in that it targets the United States and its allies across the globe and pursues broad geopolitical aims. Although the U.S. campaign against al-Qaeda and the global jihadist movement campaign had some notable successes, such as the destruction of al-Qaeda's sanctuary in Afghanistan, the elimination of many of the group's leaders, and the growing resolve of many countries to take action against al-Qaeda and its associates, no informed observers believe that al-Qaeda will be eliminated anytime soon. The United States itself continues to be threatened by large-scale attacks, as suggested by heightened security alerts and reports of plans to attack financial targets in New York and Washington. Countering al-Qaeda is thus likely to preoccupy U.S. national security institutions for at least the remainder of the decade, and perhaps longer. This study explores some of the most salient aspects associated with terrorist phenomena across the world and their implications for the security of the United States and its friends and allies. The results of the study are reported in two volumes: The subject of this first volume is al-Qaeda and what we refer to as the "al-Qaeda nebula," an ecosystem of terrorist groups around the world that have internalized the al-Qaeda worldview and its methodology of mass-casualty terrorist attacks.

0315 **Downing, Wayne A.,** ***Al-Qaida's (Mis)Adventures in the Horn of Africa,*** **Combating Terrorism Center, U.S. Military Academy, January 2007. 228pp.**

Based on a collection of al-Qa'ida documents recently released from the Department of Defense's Harmony Database, this report provides an analysis of al-Qa'ida's early operations in the Horn of Africa. These documents, captured in the course of operations supporting the Global War on Terror, have never before been available to the academic and policy community. Al-Qa'ida's (mis)Adventures in the Horn of Africa includes a theoretically informed analysis of al-Qa'ida's successes and failures while operating in Somalia between 1992 and 1994. Case studies on Somalia and Kenya provide a historical and current analysis of al-Qa'ida's operations in the Horn. Our theoretical analysis and case studies inform policy recommendations on how the U.S. and its coalition partners might address the threat of terrorism in failed and weak states within the Horn of Africa and globally. We have provided brief summaries of each of the released documents with full text translations in English and the original document in Arabic. We hope this report will serve as a useful resource in our collective efforts to better understand and combat al-Qa'ida and its affiliated movements.

0544 **Blanchard, Christopher M.,** ***Al Qaeda: Statements and Evolving Ideology,*** **Congressional Research Service, Library of Congress, January 24, 2007. 19pp.**

Osama Bin Laden and the Al Qaeda terrorist network have conducted a sophisticated public relations and media campaign over the last 10 years. Terrorism analysts believe that these messages have been designed to elicit psychological reactions and communicate complex political messages to a global audience as well as to specific populations in the Islamic world, the United States, Europe, and Asia. Some analysts believe that Al Qaeda's messages

contain signals that inform and instruct operatives to prepare for and carry out new attacks. Bin Laden has referred to his public statements as important primary sources for parties seeking to understand Al Qaeda's ideology and political demands. Global counterterrorism operations in the aftermath of the September 11, 2001 terrorist attacks appear to have limited Bin Laden's ability to provide command and control leadership to Al Qaeda operatives and affiliated groups. Other Al Qaeda leaders continue to release statements that sanction, encourage, and provide guidance for terrorist operations. Iraq has become a focal point for Al Qaeda's rhetoric, and statements continue to underscore Al Qaeda leaders' interest in Iraq and support for the ongoing insurgency. Statements released by Bin Laden and his deputy Ayman Al-Zawahiri since late 2004 have rekindled public debate in Europe and the United States surrounding Al Qaeda's ideology, motives, and future plans for attacks. Statements released following the July 2005 Al Qaeda-linked suicide bombing attacks on the London transit system have characterized those attacks and Al Qaeda's ongoing terrorist campaign as a response to British and U.S. military operations in Iraq. This report reviews Al Qaeda's use of public statements from the mid-1990s to the present and analyzes the evolving ideological and political content of those statements. The report focuses on statements made by Osama Bin Laden, his deputy Ayman Al-Zawahiri, Abu Musab Al Zarqawi, and Sayf Al Adl.

0563 **Porterfield, Robin, *The GWOT Evolution: Has the United States Opened Pandora's Box?*, U.S. Army War College, March 30, 2007. 19pp.**

The war on terrorism was the battle cry sounded by the United States in response to the events of 9/11. The enemy in this war was different than any the United States had faced before. The threat posed by al Qaeda and the radical ideology it inspired required changing how the United States would approach problems and issues in the future. Unfortunately, instead of changing its strategy to fit the problem, the United States changed the problem to fit its known strategies. The war on terrorism evolved into a war on rogue states and weapons of mass destruction, the foreign policy approach the United States was pursuing before 9/11. This evolution gave the impression that the U.S. was overstepping its legal and moral authority. Support for the United States dropped significantly, both internationally and domestically. At issue is the question, has the U.S. opened up the proverbial “Pandora's Box” by expanding the war on terrorism beyond terrorists and their ideology? What impact will this have on U.S. interests and influence in the world? This paper explores these questions and reveals that a refocusing of the U.S. foreign policy is required into the next century.

0582 **Hoag, Lyle, *Give Deterrence a Chance: A Strategy Against Al Qaeda*, U.S. Army War College, March 30, 2007. 27pp.**

Engaged in a global war on terrorism, America is fighting in Iraq and Afghanistan to rid the world of Al Qaeda, other apocalyptic terrorists, and the regimes that harbor them. In the National Strategy for Combating Terrorism, the president has laid out a strategy to defeat these terrorists. While deterrence is contained in the strategy, it is apparent from the application of the strategy that deterrence has not been used or that its use is effective. In application, the strategy has been heavy on defeat and light on deter. It relies on the military, but does little to weave all other aspects of national power to help solve the problem of terrorism. Deterrence has many short comings as a strategy in application against terrorism but these problems can be overcome. This paper discusses deterrence and terrorism and provides a strategic framework for its use.

0609 **Chan, Wing Kai, *Defeating the Logic of Islamist Terrorism*, U.S. Army War College, March 30, 2007. 19pp**.

War is fought in the dual realm of a physical and psychological battleground. In the global war on terrorism, victory entails winning both the battle of arms and the battle of ideas. Physical destruction of the terrorist organization is an essential but insufficient condition to defeat the Islamist terrorist ideology. The war must be waged at the level where it matters, by attacking the logic of Islamist terrorism, by exposing its religious pretensions, and by undermining its popular appeal, recognizing that terrorism as a method of choice is a double-edged sword for the extremists. This internal struggle would have to be waged by moderate Muslims. While non-Muslims have no real standing in this debate, adjustments to the U.S. approach to foreign policy in the Middle East would be an important enabler for moderate Muslims. A change in foreign policy would improve the United States' image and bring about tangible changes to Muslim societies in the region. The battle of ideas is concurrently a battle of will and resolve. The current partisan disharmony in the United States must be reconciled. In the marathon to defeat the logic of Islamist terrorism, unity of purpose and effort are the prerequisites for success.

0628 **Geisler, Rudolph K., *A Global Insurgency, or Something More?* U.S. Army War College, March 30, 2007. 24pp**.

With the Global War on Terror (GWOT) beginning its sixth year and insurgencies evident in various regions across the globe, the underlying question is: are we fighting one global insurgency or isolated insurgent and/or terrorist organizations? The purpose of this paper is to explore the answer to that question. It reviews a sampling of terrorist/insurgency organizations operating worldwide and explores their ideologies and methodologies. Once this baseline is established, the argument is made that Al Qaeda is an insurgency with a global reach. However, the current world situation mandates a broader view than the myopic focus currently being given to a potential radical Islamic jihad.

0652 **Rotzien, Chad M., *Fighting a Global Insurgency Utilizing Galula's Counterinsurgency Warfare Theory*, U.S. Army War College, March 30, 2007. 20pp.**

The world in the twenty-first century has become a very dangerous place. In order to defend ourselves from those that wish to harm us and our way of life, we must clearly understand the nature of "the long war" and how to fight successfully to defeat our enemies. Many experts and politicians claim we are fighting a global war on terrorism. This is simply not true. The goal of these non-state actors is to get the United States, and the rest of the Western World, to succumb to their demands, their ideology and eventually, their way of life. We are in the midst of a global insurgency, and the best way to counter this insurgency is to employ the counterinsurgency warfare theory of David Galula, apply it to a global stage, and adapt it to fit the nature of this insurgency. The following strategy research project will define insurgency and the nature of insurgencies. Then, it will outline Galula's counterinsurgency warfare theory by reviewing his strategy, operations and tactics. And finally, it will explore some of the underlining causes of insurgencies and how to apply Galula's counterinsurgency warfare theory to the conflicts we face in the twenty-first century.

0672 **Boudali, Lianne Kennedy, *The GSPC: Newest Franchise in al-Qa'ida's Global Jihad,* Combating Terrorism Center, U.S. Military Academy, April 2007. 10pp.**

The GSPC, one of the most notorious terrorist groups in North Africa, has aligned with Al Qaida and changed its name to The Organization of al Qaida in the Land of the Islamic Maghreb. Some observers have speculated that North Africa may be the next safe haven for al Qaida, and that European countries may face a greater risk of attack if Algerian terrorist groups expand their base of support in Europe. The alignment of the GSPC with al Qaida represents a significant change in the group's strategy, however, its decision to join al Qaida's global jihad should be understood as an act of desperation. The Groupe Salafist pour la Prdication et le Combat (GSPC) was founded in 1998 as an offshoot of the Armed Islamic Group (GIA). The GIA was one of the strongest and most violent groups fighting the Algerian government in a civil war that killed over a hundred thousand civilians.

0682 **Kapusta, Philip E., *Suicide Bombers in CONUS,* U.S. Army Command and General Staff College, May 7, 2007. 116pp.**

This monograph analyzes post-1980 suicide bombings and determines the probability of such bombings occurring in the Continental United States (CONUS). The analysis includes a brief history of modern suicide bombing; an examination of the strategic, tactical, social, and individual logic of suicide bombing; a discussion of the probable characteristics of suicide bombings against the United States, both within CONUS and abroad; and recommendations about what can be done to mitigate future bombings. Suicide attackers have been a part of warfare for over two millennia, but the coupling of suicide attackers and explosives greatly increased the importance and effectiveness of this tactic in the 20th century. The modern phenomenon of suicide bombing had its genesis in the Iran-Iraq War from 1980-88. Concurrent with the Iran-Iraq War, Iran influenced the development of Hezbollah in Lebanon. Hezbollah tried suicide bombing against the United States and France, and then later against Israel. Other groups such as the Liberation Tigers of Tamil Eelam (LTTE), the Palestinians, and the People's Liberation Army of Kurdistan (PKK) started employing suicide bombers in the 1980s and 1990s. As suicide bombing spread geographically and ideologically, it also increased in sophistication. It advanced from being a simple bomb delivered by truck, to include suicide vests, boat bombs, and eventually airplanes. The vast majority of suicide bombings (98%) are part of an organized campaign. The only group that conducts suicide bombings against the United States outside of active war zones is Al-Qaida. Al-Qaida attacks have evolved to the point where there are two different strains: al-Qaida-sponsored and al-Qaida-inspired. Both are likely to occur in the continental United States within the mid-future.

0799 **Greenbaum, Rebecca L., *The Impact of Television News Coverage on Al-Qaeda's Operations,* Naval Postgraduate School, June 2007. 93pp.**

Much of what the American public knows about al-Qaeda and its most prominent member, Osama bin Laden, has been delivered through television news. It remains clear that al-Qaeda uses television news as an integral part of achieving their overarching goal, but whether television news has a reciprocal effect on al-Qaeda's future operations remains unclear. An analysis will be conducted to determine if the timing of al-Qaeda's operations coincide with an increase or decrease in public awareness of the terrorist organization based on the volume of television news coverage both the organization and its founder receive. This analysis will

be conducted in three distinct parts. First, a timeline of al-Qaeda's terrorist attacks will be created. This timeline will cover the period from the 1998 United States embassy bombings through December 2006. Although Osama bin Laden officially formed al-Qaeda in 1988, they did not appear in CNN transcripts until 1998. Five particular attacks were chosen to study the trends between large-scale events: the 1998 United States embassy bombings, the 2000 attack on the USS Cole, the attacks of 9/11, the 2004 bombings in Madrid, and the 2005 bombings of the London subway. Second, a timeline of the television news coverage by CNN will be created using the searchable news stories database, Nexis.com. This analysis will focus on the CNN television news coverage of both al-Qaeda and Osama bin Laden. A search will be conducted for each term by month and the volume of CNN news transcripts mentioning these search terms will be compiled. The goal of this data collection is to analyze the raw number of times the search terms are mentioned in television news coverage each month. The third part consists of mapping the volume of television news coverage along the timeline of al-Qaeda attacks and analyzing their interaction. The existence of trends may give insight into the timing of future attacks.

0891 **Wilson, Sean P.,** ***The Evolution of Al Qaeda,*** **U.S. Army Command and General Staff College, June 16, 2007. 134pp.**

Al Qaeda is a significant threat to the national security of the United States and its allies. This makes it important for individuals in these countries, both military and civilian, to understand the evolution of this threat. This thesis analyzes Al Qaeda's evolution from 1989 to 2006. Despite numerous assaults by the United States and its allies, Al Qaeda has evolved to continue its jihad. However, the War on Terror is not the only factor that influenced its evolution. Al Qaeda is a product of the forces of globalization. Increasing access to global finances, international travel, and sophisticated technology is what has enabled Al Qaeda to evolve into its current form. The conclusion is that Al Qaeda's evolution has made it a more formidable opponent.

REEL 14

Al-Qaeda cont.

0001 **Fitzgerald, James H., III,** ***Changing the Winds of Paradise: Confronting Al Qaeda's Ideology of Martyrdom,*** **U.S. Army Command and General Staff College, June 16, 2007. 118pp.**

Suicide terrorism is remerging as the dominant tactic in asymmetric warfare. Al Qaeda in association with affiliates in the greater Salafi-jihadi movement conduct suicide terror or martyrdom campaigns against strategic and operational targets. Martyrdom operations are the keystone of Al Qaeda's ideology and serve as a unifying tenet of the global Salafi-jihadi insurgency. This study will examine the Global War on Terrorism (GWOT) within the context of a transnational or global insurgency fueled by an extreme Islamic ideology propagated by Al Qaeda; seek to correlate the relationship between Al Qaeda's 'martyrdom operations' and radical Islamic doctrinal principles and understand the differences between strategic 'martyrdom operations' against the 'far enemy' exemplified by the attacks of 11 September 2001, and the operational martyrdom operations conducted in Iraq to facilitate the collapse of the state. The analysis highlights the threat Al Qaeda and Associated Movements

through the insurgency pose to the US and its interests. Salafi-jihadi organizations demonstrate the intent of attacking US interest and more ominously, the capability with a martyrdom campaign. Success in the GWOT depends on neutralizing the multifaceted impact of Al Qaeda's martyrdom operations.

0119 **Fishman, Brian, T*he Imaginary Emir: Al-Qa'ida in Iraq's Strategic Mistake*, Combating Terrorism Center, U.S. Military Academy, July 18, 2007. 4pp**

On July 18, 2007, General Kevin Bergner confirmed suspicions that the "Emir" of the Islamic State of Iraq (ISI)—Abu Umar al□Baghdadi—is fictitious. The information was provided by Khalid al-Mashadani, who was the Minister of Information within the ISI before he was captured by U.S. forces on July 4, 2007. If al-Mashadani's information is accurate, the al-Baghdadi deception underscores the fact that Al-Qa'ida in Iraq (AQI) made a major strategic mistake when it established the ISI in October 2006. To exploit this mistake, the United States should not simply attack the AQI/ISI organization in Iraq, but rather highlight the ISI's ideological failures.

0123 **Felter, Joseph H., *Cracks in the Foundation: Leadership Schisms in Al-Qa'ida, 1989-2006*, Combating Terrorism Center, U.S. Military Academy, September 2007. 75pp.**

Based on a collection of al-Qa'ida documents recently released from the Department of Defense's Harmony Database this report analyzes the history of al-Qa'ida's internal and long-running debates over the strategies and larger goals of the jihadi movement. Many of these documents, captured in the course of operations supporting the Global War on Terror, have never before been available to the academic and policy community. Cracks in the Foundation includes a richly sourced account of the ongoing struggle between different factions among al-Qa'ida's leaders and specific recommendations for effectively exploiting weaknesses arising from these internal struggles. Brief summaries of each of the released documents have been provided, and the full texts of the released documents can be accessed via hyperlinks within the report, both in their original Arabic and in English. This report will serve as a useful resource in the collective efforts to better understand and combat al-Qa'ida and its affiliated movements.

0198 **Felter, Joseph H., and Brian Fishman, *Al-Qa'ida's Foreign Fighters in Iraq: A First Look at the Sinjar Records*, Combating Terrorism Center, U.S. Military Academy, December 2007. 31pp.**

On December 4, 2007 Abu Umar al-Baghdadi, the reputed Emir of al-Qa'ida's Islamic State of Iraq (ISI), claimed that his organization was almost purely Iraqi, containing only 200 foreign fighters. Twelve days later, on December 16, 2007, Ayman al-Zawahiri urged Sunnis in Iraq to unite behind the ISI. Both statements are part of al-Qa'ida's ongoing struggle to appeal to Iraqis, many of whom resent the ISI's foreign leadership and its desire to impose strict Islamic law. In November 2007, the Combating Terrorism Center received nearly 700 records of foreign nationals that entered Iraq between August 2006 and August 2007. The data compiled and analyzed in this report is drawn from these personnel records, which was collected by al-Qa'ida's Iraqi affiliates, first the Mujahidin Shura Council (MSC) and then the Islamic State of Iraq (ISI). The records contain varying levels of information on each fighter, but often include the fighter's country of origin, hometown, age, occupation, the name of the fighter's recruiter, and even the route the fighter took to Iraq. The records were

captured by coalition forces in October 2007 in a raid near Sinjar, along Iraq's Syrian border. Although there is some ambiguity in the data, it is likely that all of the fighters listed in the Sinjar Records crossed into Iraq from Syria.

0229 **Hurst, Cindy, *The Terrorist Threat to Liquefied Natural Gas: Fact or Fiction?* Institute for the Analysis of Global Security, February 2008. 16pp.**

On 14 February 2007, the Saudi Arabian arm of al-Qaeda put out a call to all religious militants to attack oil and natural gas sources around the world. Through such attacks, according to the call, al-Qaeda hopes to "strangle" the U.S. economy. Such proclamations give fodder to those who highlight the possibilities that liquefied natural gas (LNG) could be used as a lethal weapon of mass destruction. Industry officials on the other hand point out the improved security measures in place as a result of 9/11. Proponents of natural gas are correct in that both safety and security measures currently in place make LNG terminals and ships extremely hard targets for terrorists. However, it would be imprudent to believe that terrorists are either incapable or unwilling to attack such targets. It would be equally imprudent to assume that these targets are impenetrable. If anything, in today's environment, insiders will always remain a potential threat. Few groups are capable of implementing an attack on LNG. However, an attack on LNG would fit well with al-Qaeda's tactics, techniques and procedures. The most inherent problem with LNG is that despite scientists, scholars, officials and academicians conducting various high profile studies on the safety implications of LNG, too many unknown variables and unanswered questions still exist. Experts don't agree fully on safety boundaries. Empirical data demonstrating what would happen if there was to be an attack are virtually non-existent. Because of this uncertainty, members of the public remain adamantly opposed to bringing LNG with its foreign ships and crews into their backyards, perhaps rightly so. More studies are needed to bring about sound conclusions and ensure the greatest possible degree of public safety, as well as to ensure the security of an important commodity.

0245 **Hancock, Daniel Adam, *The Olive Branch and the Hammer: A Strategic Analysis of Hawala in the Financial War on Terrorism*, Naval Postgraduate School, March 2008. 93pp.**

Since September 11, 2001, U.S. counter-terror efforts to disrupt al Qaeda's finances have been imprecise at best; at worst, they have had profound negative effects. The question of why hawala poses such a great threat and why there is a need for strict regulation or elimination of hawala has been the subject of great deliberation among policy makers and financial scholars since al Qaeda's attack on New York and Washington, D.C. The purpose of this thesis is to understand the complexities of the hawala informal financial transfer system prevalent in the Middle East and assess its complicity with terrorist financing. To that end, this thesis examines whether the hawala system itself pose a significant terrorist threat to the United States as a medium for financial transactions for terrorist organizations. By conducting a detailed analysis of hawala in Afghanistan from 2001-2006, this thesis provides a framework to assess whether the hawala system poses a strategic threat in the U.S. led war on terror. Furthermore, by studying regulation attempts in Afghanistan, this thesis examines the cultural and economic effects of U.S. efforts on Muslims.

0339 **Gastal, Piotr, *Targeting Civilians with Indiscriminate Violence*, Naval Postgraduate School, March 2008. 107pp.**

Terrorist violence against innocent people in Iraq continues despite the determination of Coalition and Iraqi forces to stop it. This thesis examines the relationship between a terrorist organization's strategy of using indiscriminate violence to attack the civilian population and its operational success. Specifically, the tactic to be examined is that of the al Qaeda in Iraq, which has attacked civilians with indiscriminate violence (in the context of the insurgency) since the formal termination of hostilities in Iraq in May 2003. Using the historical example of the insurgency in Algeria, 1992-1999, this thesis hopes to find the answer as to whether, and under what conditions, terrorist tactics of attacking civilians with indiscriminate use of violence applied by Iraqi Islamist insurgents may be effective in reaching their political aims. Also, this thesis will question whether this manipulation of violence can turn the population against the protagonists, rather than mobilizing it in favor of one of them. The thesis will answer the question of why Islamist insurgents from al Qaeda in Iraq kill civilians in unjustifiable ways: slaughtering, decapitating, bombing and shooting hundreds of men, women and children.

0445 **Christensen, Leslie L., *Preparing for the Next Kamikaze Attack on the American Homeland*, U.S. Army War College, March 15, 2008. 26pp.**

This paper presents a case for not diverting additional Transportation Security Administration (TSA) resources from Civil Aviation security to General Aviation (GA) security. It acknowledges that the TSA spends very little on GA security even though Al-Qaeda retains the capability to conduct strategic attacks using GA aircraft. In developing the argument against diverting resources, the author reviews three reasons why Al-Qaeda will not use GA aircraft in a strategic strike against the U.S. Firstly, other methods are available that are both easier to execute and would cause more damage than a GA attack. Secondly, attacking the U.S. homeland is against Al-Qaeda's operational interests because doing so would bring the American people back into the fight. Finally, attacking the U.S. homeland is against Al-Qaeda's operational interests because doing so would reverse its successes in gaining international support for the removal of U.S. forces from Iraq. Because Al-Qaeda will not strike the U.S. homeland using GA aircraft, TSA should not divert additional resources from Civil Aviation security to General Aviation security.

0471 **Graves, Thomas C., *Al Qaeda, RMA, and the Future of Warfare*, U.S. Army War College, March 15, 2008. 32pp.**

As a result of the end of the Cold War, the fall of the Soviet Union, US success during the Gulf War, and other factors, the US military reduced its size in the 1990s. Concurrently, the US military pursued a revolution in military affairs (RMA) in an effort to offset the reduction in size by gaining efficiency through the application of new technology, techniques, and doctrine. This monograph examines these efforts and draws a comparison between the US efforts in the 90s and the rise of Al Qaeda as a non-state, terrorist, organization. Using Napoleonic warfare and Blitzkrieg as models of RMA, the monograph draws parallels between Napoleon and Al Qaeda and Blitzkrieg and the US military. It identifies the US efforts on RMA as focused at the tactical and operational levels of war while Al Qaeda focused at the strategic level of war. The monograph finishes with recommendations on the future of US efforts at transformation; specifically with regards to integrating all elements of

national power and restructuring the interagency process in order to respond to the concept of RMA as advanced by Al Qaeda.

0504 **Bozzelli, Joseph P.,** ***The Suitability of Defector Operations Applied Against Al Qaeda,*** **U.S. Army Command and General Staff College, March 19, 2008. 49pp.**

During the Vietnam conflict the United States along with the South Vietnam government were able to convince 194,000 enemy personnel to change sides. The majority of these individuals were then exploited for intelligence, propaganda, and other capabilities beneficial to the allies and detrimental to the communist cause. The United States has a long history of using defector operations stretching back to the War of Independence and on through to the end of the Cold War. In spite of this history of experience there is barely a mention of defector operations in modern unclassified doctrine; nor, more importantly, have defector operations been employed as a weapon against Al Qaeda. With common characteristics and a common objective, common Lines of Operations can be established for insurgencies. These insurgency Lines of Operations are: Information Operations, Secrecy, Establishing Safe Base of Operations, Establishing Support, Gaining New Members, and Creating and Maintaining an Internal Structure. By studying both the previous application of defector operations and the academic study on the subject the Lines of Capabilities for defector operations were established. These Lines of Capability are: Intelligence, Psychological Operations, Government Legitimacy, Counterinsurgency Force Enhancement, and Insurgent Instability. When these Lines of Capability are overlaid onto Al Qaeda's Lines of Operations, specific points of impact can be determined. When these points of impact are extrapolated upon it can be established that defector operations would be a suitable program for use against Al Qaeda.

0553 **Brachman, Brian Fishman, and Joseph Felter,** ***The Power of Truth: Questions for Ayman al-Zawahiri,*** **Combating Terrorism Center, U.S. Military Academy, April 21, 2008. 27pp.**

On 16 December 2007, Ayman al-Zawahiri invited journalists and Jihadist enthusiasts to ask him questions via the primary Jihadist web forums. Zawahiri promised to personally answer some of those questions in a subsequent statement. On 2 April 2008, As-Sahab Media released the first part of Zawahiri's response in the form of a one hour, forty-three minute audio statement, which was accompanied by Arabic and English transcripts. Zawahiri used the opportunity to publicly address topics that have been dogging him for years. He answered some questions directly, like whether al-Qa'ida's willingness to kill innocent Muslims in the course of their operations is apostasy. He sidestepped other questions, including more politicized ones about al-Qa'ida's increasing difficulties in Iraq and, in particular, al-Qa'ida's official position toward Iran. The Power of Truth? is the CTC's assessment of Ayman al-Zawahiri's 2 April 2008 response to his solicitation for questions.

0580 **Hanratty, Martin,** ***Can the United States Defeat Radical Islam?*** **U.S. Army Command and General Staff College, May 22, 2008. 159pp.**

On September 11, 2001, Al-Qaeda and affiliated jihadist organizations declared war on the United States. Since that day, the U.S. government has initiated a series of policies, legislation and actions to confront the new threat. There is growing criticism of the structure and approach the U.S. has adopted to defeat Al-Qaeda and the Salifist jihad organizations that support it. This monograph explores the basis of this criticism and determines whether or

not the United States has the institutional structure, human resources and polices required to project the full complement of diplomatic, military, intelligence resources required to defeat Al-Qaeda and the global Salafist jihad that it represents. The monograph tracks changes in U.S. legislation, organizational structure, and actions mounted to contain and defeat Al-Qaeda since the 9/11 attacks. It presents non-classified evidence regarding the effectiveness of these changes to identify, interdict and neutralize Al-Qaeda and its affiliated groups and records how Al-Qaeda has responded. The monograph concludes with a set of recommended strategic and global adjustments to the U.S. global war on terrorism required to defeat Al-Qaeda and its affiliated terrorist network. The monograph opens with an evaluation of Al-Qaeda's origins and cause, its recruiting base and methods, its cellular structure and operating procedures, and its financial assets including the sources of its funding, how funds are moved and managed, and how these funds are used to support the global Salafist jihad that Al-Qaeda embodies. This is followed by an analysis of the U.S. government structure and capabilities available to meet the challenged posed by Al-Qaeda prior to the 9/11 attacks. The monograph then turns to examine both the short and long-term responses of the U.S. government to the attacks.

0741 **Charles, Andrew J.,** ***Preempting and Countering Al Qa'ida's Influence: Development of a Predictive Analysis and Strategy Refinement Tool,*** **U.S. Army Command and General Staff College, June 13, 2008. 139pp.**

From shortly after its inception, Al Qaida has sought sanctuaries from which it could safely operate and provide support to Islamist groups around the world. It found one in Sudan from 1992 to 1996, in Afghanistan from the late 1980s to 2001, and in northern Pakistan in the 1980s, 1990s, and even after 2001. It also sought a sanctuary in Somalia in the early 1990s but had only limited success due to a number of societal factors. Operation Enduring Freedom ousted Al Qaida from its Afghani safe haven, forcing it to find a secure environment elsewhere. Initially that place was in northern Pakistan, but Al Qaida undoubtedly will search for other areas to expand its influence as international influences pressure the Pakistani government to allow more and more operations into the northern provinces. This thesis develops and validates a hypothesis that identifies eight characteristics of a society that attract Al Qaida and help them establish a secure environment from which to operate. The characteristics defined in this hypothesis will aid in predicting Al Qaida's future engagement endeavors and help develop more tailored, poignant engagement strategies to preempt or counter Al Qaida's expansion efforts.

0880 **Fishman, Brian,** ***Bombers, Bank Accounts & Bleedout: Al-Qa'ida's Road In and Out of Iraq*****, Combating Terrorism Center, U.S. Military Academy, July 22, 2008. 126pp.**

This report is the second by the Combating Terrorism Center to assess the demographics, procedures, finances, and leadership of al-Qa'ida's foreign fighters, especially those currently fighting in Iraq. This report analyzes al-Qa'ida in Iraq's (AQI) operations from spring 2006 to summer 2007 and is being issued with a trove of AQI documents captured by coalition forces near Sinjar, Iraq. The documents include almost 600 AQI personnel records for foreign fighters crossing into Iraq, AQI contracts for suicide bombers, AQI contracts for fighters leaving Iraq, narratives written by al-Qa'ida's Syrian smugglers, and AQI financial records. The CTC also acquired demographic information on all Third Country Nationals (TCNs) in detention at Camp Bucca, Iraq. Most of this data has not previously been released to the public.

1006 **Aboul-Enein, Youssef, *The Late Sheikh Abdullah Azzam's Books, Part I: Strategic Leverage of the Soviet-Afghan War to Undertake Perpetual Jihad,* Combating Terrorism Center, U.S. Military Academy, [no month] 2008. 11pp.**

Sheikh Abdullah Azzam, more than any other cleric, is considered the strategic founder of al-Qaida. His calling to establish an "al-Qaida al-Sulba" (firm foundation) to export jihad where Muslims are being persecuted is the name Bin Laden finally chose when naming his organization "al-Qaida." To understand Bin Laden and those who harbor sympathies toward al-Qaida it is vital to rediscover Azzam's books. Part I of this series looks into a book published in 1984, which by 1988 had gone through its 11th printing. Azzam's Quranic interpretations of the Soviet-Afghan War and his mythologizing and marketing of this conflict was a means to attract more Arabs to join the fight. The book is entitled *Ayyat al-Rahman fee Jihad al-Afghan* (*God's Signs in the Afghan Jihad*).

1017 **Aboul-Enein, Youssef, *The Late Sheikh Abdullah Azzam's Books, Part II: Remedy for Muslim Victimization,* Combating Terrorism Center, U.S. Military Academy, [no month] 2008. 9pp.**

Sheikh Abdullah Azzam, more than any other cleric, is considered the strategic founder of al-Qaida. His calling to establish an "al-Qaida al-Sulba" (firm foundation) to export jihad where Muslims are being persecuted is the name Bin Laden finally chose when naming his organization "al-Qaida." To understand Bin Laden and those who harbor sympathies toward al-Qaida it is vital to rediscover Azzam's books. Part II of the series explores a book on Azzam's views regarding the remedy for Muslim victimization.

1026 **Aboul-Enein, Youssef, *The Late Sheikh Abdullah Azzam's Books, Part III: Radical Theories on Defending Muslim Land through Jihad,* Combating Terrorism Center, U.S. Military Academy, [no month] 2008. 13pp.**

Sheikh Abdullah Azzam, more than any other cleric, is considered the strategic founder of al-Qaida. His calling to establish an "al-Qaida al-Sulba" (firm foundation) to export jihad where Muslims are being persecuted is the name Bin Laden finally chose when naming his organization "al-Qaida." To understand Bin Laden and those who harbor sympathies toward al-Qaida it is vital to rediscover Azzam's books. Part III looks at Azzam's history and his theories of what needs to be done to defend Muslim lands that are under assault.

REEL 15

Bioterrorism

0001 **Bentson, Kjirstin A., *An Epidemiological Approach to Terrorism,* U.S. Air Force Institute of Technology, March 2006. 130pp.**

There are many types of models for counterterrorism, explaining different problems that the military faces in the fight against terrorism. This thesis proposes that one of the fundamental assumptions underlying existing models of counterterrorism is that the struggle with terrorists can be understood as a war in the traditional sense of the term. This paper proposes

to rethink the struggle against terrorism as a fight against an infection. The epidemic of terrorist ideology within part of the world is a result, from this perspective, of the infectiousness of that ideology. Using the insights of the field of the epidemiology of ideas, this research looks into the models and methods used to understand and fight biological epidemics. The paper utilizes the SIR model from mathematical epidemiology, which partitions populations into susceptible, infected, and recovered categories, and apply that model with notional starting rates to the epidemic of terrorist ideology. This research allows another set of assumptions for models used in counterterrorism because the insights gained from viewing terrorism as a symptom of an epidemic can expand our understanding of the problem that we fight.

0131 **Schacht, Wendy, and John R. Thomas, *Bioterrorism Countermeasure Development: Issues in Patents and Homeland Security*, Congressional Research Service, Library of Congress, November 27, 2006. 25pp.**

Congressional interest in the development of bioterrorism countermeasures remains strong, even after passage of legislation establishing Project BioShield. Several bills considered, but not enacted during the 109th Congress, including S. 3, the Protecting America in the War on Terror Act of 2005; S. 975, the Project Bioshield II Act; and S. 1873, the Biodefense and Pandemic Vaccine and Drug Development Act, would have generated additional incentives for the creation of new products and processes by the private sector to counteract potential biological threats. These bills proposed reforms to current policies and practices associated with intellectual property, particularly patents, and the marketing of pharmaceuticals and related products. Patents appear to be important in the promotion of innovation, particularly in the pharmaceutical sector. This report explores the role of patents in encouraging the development and commercialization of new inventions and discusses the relationships between patent ownership and the generation of biomedical products. However, the grant of a patent on a pharmaceutical does not permit marketing of the product without the approval of the Food and Drug Administration (FDA). Thus, this report also examines policies concerning the use of FDA marketing exclusivity as an additional incentive to industry research and development (R&D) in this arena. Current law and suggested legislative changes are discussed to provide a context for any further exploration of related issues during the 110th Congress.

0156 **Levi, Jeffrey, *Ready or Not? Protecting the Public's Health from Diseases, Disasters, and Bioterrorism, 2006*, Trust for America's Health, December 2006. 55pp.**

The *Ready or Not?* report contains state-by-state health preparedness scores based on 10 key indicators to assess health emergency preparedness capabilities. All 50 U.S. states and the District of Columbia were evaluated. Half of states scored six or less on the scale of 10 indicators. Oklahoma scored the highest with 10 out of 10; California, Iowa, Maryland, and New Jersey scored the lowest with four out of 10. States with stronger surge capacity capabilities and immunization programs scored higher in this year's report, since four of the measures focus on these areas.

0211 **Walter, Katie, *An Action Plan to Reopen A Contaminated Airport*, Lawrence Livermore National Laboratory, December 2006. 3pp.**

How would authorities respond if San Francisco International Airport (SFO) were to be contaminated with anthrax, and how long would it take to restore the airport to full usability? An intentional bioterrorist attack at the airport could endanger the health of hundreds of people. Long-term closure of this critical transportation hub during decontamination would have disastrous effects on the regional and national economy. With that experience in mind, the Department of Homeland Security (DHS) funded a project to minimize the time a major transportation facility would be closed following a biological attack. Lawrence Livermore and Sandia national laboratories led the project, in partnership with SFO, to develop response and restoration protocols for such events. The group's work culminated in January 2006 when 120 officials from local, state, and federal agencies participated in a two-day demonstration at SFO's old international terminal to test the new procedures.

0214 **Thompson, Christopher M., *The Bioterrorism Threat by Non-State Actors: Hype or Horror?* Naval Postgraduate School, December 2006. 109pp.**

This thesis provides a capabilities-based approach to assessing the bioterrorism threat from non-state actors. Through comparative case study, prior bioterrorism attacks are analyzed to assess capability in the three areas necessary to complete a biological weapons attack: obtaining or isolating a pathogen, weapon-izing the agent, and employing or disseminating the weapon. The three cases are the Rajneeshee cult in 1984, the Aum Shinrikyo cult in the early 1990s, and the United States Postal System anthrax attacks of 2001. In contrast to current wisdom that employing biological weapons is too difficult for non-state actors, this thesis reveals a broad spectrum of capability in all studies in the areas necessary to culminate an attack. Application of these findings must be used to assess risk generally rather than against specific groups because capability is deemed to be extremely difficult to track. The thesis finds that a significant threat exists, but it is not large enough to be over-hyped above other national security concerns. In light of this, recommendations are provided for U.S. bio-defense policy emphasis in the areas of the nonproliferation regime, attribution capabilities, and defending against the changing nature of future attacks with a particular emphasis on the public health system.

0323 **Burgess, Lawrence P., *Bioterrorism Preparedness for Infectious Disease (BTPID) Proposal*, U.S. Army Medical Research and Material Command, January 2007. 102pp.**

Bioterrorism preparedness for infectious disease (BTPID) as part of homeland defense initiatives continues to advance. Significant opportunities exist for new research and development of bioinformatics and telecommunications solutions for BTPID that can complement ongoing initiatives. With this in mind this funded effort with additional proposal modifications progressed from a planning study identification of problems and potential solutions analyses of potential solutions all resulting in important recommendations and knowledge. This project also helped to establish a Joint Clinical Research Center in Thailand. In addition to the effort described above an additional modification was added to the existing proposal to expand relationships with nations in Southeast Asia (SEA) which will help foster bioterrorism related infectious disease research in Thailand and SEA in general. This

modification enabled advanced simulation-based training on-site during the 2005 APMMC held in Vietnam. The project in its entirety represents a strengthening of knowledge and resources related to bioterrorism and infectious disease as well as a strengthening in Asia-Pacific relationships that are beneficial in working future problems related to bioterrorism infectious disease outbreaks and effective exchange of information. Publications resulting from certain efforts in this project also document this knowledge for application wherever it may be needed in the future. This final report summarizes the spectrum of objectives accomplishments and products from work conducted over the entire research period.

0425 **Raber, E.,** ***Summary Document: Restoration Plan for Major Airports after a Bioterrorist Attack*****, Lawrence Livermore National Laboratory, January 12, 2007. 15pp.**

This document provides general guidelines for developing a Restoration Plan for a major airport following release of a biological warfare agent. San Francisco International Airport was selected as the example airport during development of the Plan to illustrate specific details. The spore forming bacterium Bacillus anthracis was selected as the biological agent of primary concern because it is the most difficult of known bioterrorism agents to inactivate and is considered to be one of the agents most likely to be used as a biological weapon. The focus of the Plan is on activities associated with the Characterization, Remediation, and Clearance Phases that are defined herein. Activities associated with the Notification and First-Response Phases are briefly discussed in Appendixes A and B, respectively. In addition to the main text of this Plan and associated appendixes, a data supplement was developed specifically for San Francisco International Airport. Requests for the data supplement must be made directly to the Emergency Planning Operations Division of San Francisco International Airport.

0440 **Reed, Patricia Diane,** ***Integrating Local Public Health Agencies into the Homeland Security Community*****, Naval Postgraduate School, March 2007. 60pp.**

After years of funding through the Centers for Disease Control and Prevention, local public health agencies have made inconsistent progress in fulfilling their Homeland Security objectives. Most progress has been made in those areas in which Public Health has previous experience. However, in those activities requiring integration with other responder agencies Public Health has lagged in developing effective capabilities in prevention, preparedness, response, mitigation and recovery. This thesis argues that several factors contribute to this lack of success, including funding structures and guidelines, the reluctance on the part of other responder agencies to include Public Health in emergency planning and response activities, and the organizational isolation in which Public Health has existed. In order for local public health agencies to meet their Homeland Security objectives, funding structures and guidelines must support local Public Health and public health agencies must be better integrated with their Homeland Security partners. Public health agencies at all levels and their leadership have the opportunity to effect organizational changes designed to accelerate the transformational process, enhancing their Homeland Security partnerships. Public Health agencies can be more effectively integrate into the larger Homeland Security community by demonstrating commitment to making these changes.

0500 **Martinez, Coleen K., *Biodefense Research Supporting the DoD: A New Strategic Vision*, Strategic Studies Institute, March 2007. 43pp.**

This monograph examines the current organization of the DoD biodefense research program in light of the changing national biodefense landscape and industry best practices, and argues that all aspects of the DoD biodefense program should be consolidated with all other federal biodefense resources, including those within the National Institutes of Health, to create a single, focused, and productive program. This new agency, subordinate to the Department of Health and Human Services, will be positioned and equipped to provide medical solutions to the warfighter on the battlefield, as well as to U.S. citizens.

0543 **Neu, Annette L., *Building Collaborative Capacity for Biosecurity at the Georgia Seaports*, Naval Postgraduate School, March 2007. 89pp.**

When public health interventions are incorporated into a comprehensive seaport security strategy, they can effectively prevent and reduce morbidity and mortality, resulting from natural or man-made disasters. The challenge is to build collaborative capacities through new and renewed seaport surveillance activities among government agencies and private companies to strengthen the role of public health to detect, intercept, and mitigate the potential effects of the intentional or unintentional introduction of diseases. Currently, effective collaborative processes between public health agencies and other local, state and federal partners in seaport security are weak and primarily the result of informal activities. Although seaport security receives considerable policy attention in other areas of risk management, such as radiological detection, public health investments are relatively neglected. Effective, sustainable approaches to building interagency collaboration could prove to be an indispensable homeland security initiative to prepare for a bioterrorism attack or other infectious disease incidents.

0631 **Smith, Chester Lee, Jr., *Involving Corporations in Dispensing during Mass Prophylaxis*, Naval Postgraduate School, March 2007. 99pp.**

The purpose of the mass prophylaxis following a bioterrorist attack is to reduce fear within the community and to reduce loss of life to the disease. Current U.S. government guidance provided by the Department of Health and Human Services Centers for Disease Control and Prevention (CDC) for response to an anthrax attack states that the optimal amount of time for distribution of prophylaxis to the community is two days. Yet, how can the public health agencies of a state dispense antibiotics to everyone in a large metropolitan area within forty-eight hours of potential exposure? A key challenge to a successful mass prophylaxis campaign is staffing the functions required to receive, stage, transport, deliver, and dispense antibiotics. Is there value in developing relationships with large corporations within the metropolitan area to support their active involvement as reliable, effective, and efficient volunteer entities for dispensing pharmaceuticals following a terrorist incident or natural disaster? This thesis evaluates the novel approach of inviting corporations to act as volunteer entities in and of themselves (rather than merely offering their facilities for use to support a government activity) as well as more traditional options such as utilizing the current public health force (supported by traditional volunteer recruitment) and using the United States Postal Service to directly deliver medication to households. A fourth option, combining the first three options to meet the requirements of timely delivery, security, medical personnel support, nonmedical personnel support, and client information collection is also considered.

0727 **Rowe, Thomas W., *Testing the Effectiveness of the North Shore-LIJ Health System's Bioterrorism Response Program to Identified Surveillance Data,* U.S. Army Medical Research and Material Command, March 2007. 34pp.**

This research project was to measure the importance of timely notifications of potential infectious disease outbreaks, provided by electronic-syndromic surveillance system, compared to the manual case-review system.

0761 **Gottron, Frank, Project *Bioshield: Appropriations, Acquisitions, and Policy Implementation Issues for Congress,* Congressional Research Service, Library of Congress, March 8, 2007. 25pp.**

The Project BioShield Act of 2004 (P.L. 108-276) established a 10-year program to acquire civilian medical countermeasures to chemical, biological, radiological and nuclear (CBRN) agents for the Strategic National Stockpile. Provisions of this act were designed to encourage private companies to develop these countermeasures by guaranteeing a government market for successfully developed countermeasures. Both the Department of Homeland Security (DHS) and the Department of Health and Human Services (HHS) have responsibilities in this program.

0787 **Lombardi, John L., et al., *Lotus LADM Based Self-Decontaminating Surfaces,* U.S. Army Research Office, May 1, 2007. 48pp.**

Recent events have lead to new concerns about biowarfare, bioterrorism, chemical warfare and chemical terrorism. Because of the potential range of agents that could be used, a non-specific decontamination system is desirable. Of particular interest are materials whose surfaces have been modified to be self-decontaminating and self-regenerating. Other beneficial attributes are that the surfaces be self-cleaning and very light weight. U.S. Army has developed superhydrophobic coating materials.

0835 **Dunfee, David A., and Benjamin L. Hegler, *Biological Terrorism Preparedness: Evaluating the Performance of the Early Aberration Reporting System (EARS) Syndromic Surveillance Algorithms,* Naval Postgraduate School, June 2007. 145pp.**

After the terrorist attacks of September 11, 2001, questions developed over how quickly the country could respond if a bioterrorism attack were to occur. "Syndromic surveillance" systems are a relatively new concept that is being implemented and used by public health practitioners to attempt to detect a bioterrorism attack earlier than would be possible using conventional biosurveillance methods. The idea behind using syndromic surveillance is to detect a bioterrorist attack by monitoring potential leading indicators of an outbreak such as absenteeism from work or school, over-the-counter drug sales, or emergency room counts. The Center for Disease Control and Prevention's Early Aberration Reporting System (EARS) is one syndromic surveillance system that is currently in operation around the United States. This thesis compares the performance of three syndromic surveillance detection algorithms, entitled C1, C2, and C3, that are implemented in EARS, versus the Cumulative Sum (CUSUM) method applied to model-based prediction errors. The CUSUM performed significantly better than the EARS' methods across all of the scenarios evaluated. These scenarios consisted of various combinations of large and small background disease incidence

rates, seasonal cycles from large to small (as well as no cycle), daily effects, and various levels of random daily variation. This results in the recommendation to replace the C1, C2, and C3 methods in existing syndromic surveillance systems with an appropriately implemented CUSUM method.

0979 **Hu, Cecilia X., and Matthew C. Knitt, *A Comparative Analysis of Multivariate Statistical Detection Methods Applied to Syndromic Surveillance,* Naval Postgraduate School, June 2007. 95pp.**

Biological terrorism is a threat to the security and well-being of the United States. It is critical to detect the presence of these attacks in a timely manner so that emergency services can provide sufficient and effective responses to minimize or contain the damage inflicted. Syndromic surveillance is the process of monitoring public health-related data and applying statistical tests to determine the potential presence of a disease outbreak in the observed system. This research involved a comparative analysis of two multivariate statistical methods: the multivariate cumulative sum (MCUSUM) and the multivariate exponentially weighted moving average (MEWMA), both modified to look only for increases in disease incidence. While neither of these methods is currently in use in a biosurveillance system, they are among the most promising multivariate methods for this application. This analysis was based on a series of simulations using synthetic syndromic surveillance data that mimics various types of background disease incidence and outbreaks. The authors found that, similar to results for the univariate CUSUM and EWMA, the directionally sensitive MCUSUM and MEWMA perform very similarly.

1073 **Feldmesser, Marta, *Monoclonal Antibodies to Prevent Use of Mycotoxins as Biological Weapons,* U.S. Army Medical Research and Material Command, July 2007. 7pp.**

Aflatoxin exposure causes a broad range of adverse effects including acute hepatic failure hepatic carcinoma and immunosuppression. The ability to weaponize aflatoxins has already been demonstrated raising concern that these potent agents might be used for biowarfare or agroterrorism. Passive antibody therapy is used for the treatment of toxin exposures and its potential for use in the event of bioterrorism has been highlighted.

REEL 16

Bioterrorism cont.

0001 **Levi, Jeffrey, *Ready or Not? Protecting the Public's Health from Diseases, Disasters, and Bioterrorism, 2007,* Trust for America's Health, December 2007. 123pp.**

This release of the fifth annual *Ready or Not? Protecting the Public's Health from Disease, Disasters, and Bioterrorism* report, which found that while important progress has been made, critical areas of the nation's emergency health preparedness effort still require attention. In addition, the continuing trend of annual cuts in federal funding for state and local preparedness activities threatens the nation's safety. This report contains state-by-state health preparedness scores based on 10 key indicators to assess health emergency preparedness capabilities. All 50 U.S. states and the District of Columbia (D.C.) were evaluated. Thirty-seven states and D.C. scored eight or higher on the scale of 10 indicators.

Hawaii, Illinois, Kentucky, Nebraska, New Jersey, Pennsylvania, Tennessee, and Virginia scored the highest with 10 out of 10. Iowa, Mississippi, Nevada, Wisconsin, and Wyoming scored the lowest with six out of 10.

0124 **Levinson, Daniel R., *Summary Report on State, Local, Private, and Commercial Laboratories' Compliance With Select Agent Regulations,* Department of Health and Human Services, January 2008. 16pp.**

This report summarizes the results of HHS reviews of eight state, local, private, and commercial laboratories' compliance with select agent regulations during various periods from November 2003 to September 2005. This summary report was provided for CDC's use in reducing vulnerabilities at laboratories that possess, use, or transfer select agents.

0140 **Koch, Natalie, *National Decontamination Team*, Office of Emergency Management, Environmental Protection Agency, February 2008. 27pp.**

Formed in 2004, The National Decontamination Team (NDT) is a federal scientific and technical resource for decontamination science that supports actions to protect human health, the environment, and national security. NDT provides coordination, communication, and delivery of decontamination expertise to local, national, and international agencies supporting hazardous material response and remedial operations. The team consists of highly specialized and experienced emergency responders, engineers and scientists dedicated to providing immediate technical decontamination expertise at the scene of a chemical, biological, or radiological attack. NDT is a resource for expertise and support to On-Scene Coordinators (OSCs) on decontamination of buildings or other structures in the event of an incident involving releases of radiological, biological or chemical contaminants.

0167 **Department of Health and Human Services, *Biological Incident Annex*, U.S. Department of Health and Human Services, August 2008. 12pp.**

The purpose of the Biological Incident Annex is to outline the actions, roles, and responsibilities associated with response to a human disease outbreak of known or unknown origin requiring Federal assistance. In this document, a biological incident includes naturally occurring biological diseases (communicable and non-communicable) in humans as well as terrorist events. This definition also includes those biological agents found in the environment, or diagnosed in animals, that have the potential for transmission to humans (zoonosis). Incidents that are restricted to animal, plant, or food health or safety are reviewed in other annexes. Actions described in this annex take place with or without a Presidential Stafford Act declaration or a public health emergency declaration by the Secretary of Health and Human Services (HHS). This annex outlines biological incident response actions including threat assessment notification procedures, laboratory testing, joint investigative/response procedures, and activities related to recovery.

0179 **Kellman, Barry, *Biological Terrorism: U.S. Policies to Reduce Global Biothreats,* Partnership for a Secure America, September 2008. 29pp.**

This report finds progress in US government bioterrorism interdiction and response programs, and in cooperative efforts to track infectious diseases internationally, including creation of a new office charged with strengthening cooperative non-proliferation of

bioweapons and related knowledge. However, inadequate multilateral coordination and cooperation remains the single largest stumbling block to effective bioterror prevention. Despite increases in overall biothreat response funding, global threat reduction programs are still under-funded, and US disengagement from the Biological Weapons Convention has undercut the confidence necessary for effective multilateral cooperation.

0208 **Rastogi, Vipin K., et al.,** ***Surface Sampling-Based Decontamination Studies and Protocol for Determining Sporicidal Efficacy of Gaseous Fumigants on Military-Relevant Surfaces,*** **Edgewood Chemical Biological Center, September 2008. 41pp.**

A major consequence of biological terrorism in a military setting is the wide degree of contamination of combat/protective equipment used by war-fighters and first responders. Appropriate selection of a decon technology, successful implementation, and re-use of assets following decontamination rely principally on extensive pre- and post-decontamination sampling. One of the challenges related to the Test & Evaluation demonstration of decon products has been poor recovery of biological contaminants from complex surfaces. Here, we report the optimization of surface sampling for quantifying biological contaminants. An optimized surface sampling protocol was devised and used in decontamination studies for determining sporicidal efficacy of two fumigants on contaminated military-relevant surfaces.

0249 **Shea, Dana A., et al.,** ***The National Bio- and Agro-Defense Facility: Issues for Congress,*** **Congressional Research Service, Library of Congress, November 25, 2008. 29pp.**

The agricultural and food infrastructure of the United States is potentially susceptible to terrorist attack using biological pathogens. In addition to the impacts of such an attack on the economy, some animal diseases could potentially be transmitted to humans. These diseases are known as zoonotic diseases. Scientific and medical research on plant and animal diseases may lead to the discovery and development of new diagnostics and countermeasures, reducing the risk and impact of a successful terrorist attack.

0278 **Levi, Jeffrey,** ***Ready or Not? Protecting the Public's Health from Diseases, Disasters, and Bioterrorism, 2008,*** **Trust for America's Health, December 2008. 122pp.**

The report contains state-by-state health preparedness scores based on 10 key indicators to assess health emergency preparedness capabilities. More than half of states and D.C. achieved a score of seven or less out of 10 key indicators. Louisiana, New Hampshire, North Carolina, Virginia, and Wisconsin scored the highest with 10 out of 10. Arizona, Connecticut, Florida, Maryland, Montana, and Nebraska tied for the lowest score with five out of 10. Over the past six years, the *Ready or Not?* report has documented steady progress toward improved public health preparedness. This year however, TFAH found that cuts in federal funding for state and local preparedness since 2005, coupled with the cuts states are making to their budgets in response to the economic crisis, put that progress at risk.

Chemical Terrorism

0400 **Orum, Paul, *Preventing Toxic Terrorism: How Some Chemical Facilities Are Removing Danger to American Communities*, Center for American Progress, April 2006. 39pp.**

The Center for American Progress, with assistance from the National Association of State PIRGs and National Environmental Trust, conducted a survey to identify such facilities and spotlight successful practices that have removed unnecessary chemical dangers from our communities. This survey (which covered facilities that no longer report using extremely hazardous substances under the federal Risk Management Planning program) found that facilities across the country, representing a range of industries, have switched to safer alternatives from a variety of hazardous chemicals, producing dramatic security and safety benefits at a reasonable cost.

0439 **Schierow, Linda-Jo, *Chemical Facility Security*, Congressional Research Service, Library of Congress, August 2, 2006. 51pp.**

Facilities handling large amounts of potentially hazardous chemicals (i.e., chemical facilities) might be of interest to terrorists, either as targets for direct attacks meant to release chemicals into the community or as a source of chemicals for use elsewhere. Because few terrorist attacks have been attempted against chemical facilities in the United States, the risk of death and injury in the near future is estimated to be low, relative to the likelihood of accidents at such facilities or attacks on other targets using conventional weapons. For any individual facility, the risk is very small, but the risks may be increasing with potentially severe consequences for human health and the environment. Available evidence indicates that many chemical facilities may lack adequate safeguards. After 9/11, Congress enacted legislation that requires the Department of Homeland Security (DHS) to analyze vulnerabilities and suggest security enhancements for critical infrastructure. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188) and the Maritime Transportation Security Act (MTSA, P.L. 107-295) require vulnerability assessments and emergency response plans for some chemical facilities that supply drinking water or are located in ports, as well as security plans for chemical facilities in ports.

0490 **Pennington, Daniel, *Chemical Facility Preparedness: A Comprehensive Approach*, Naval Postgraduate School, September 2006. 100pp.**

Across the country thousands of facilities use, manufacture, or store large stockpiles of toxic and/or flammable substances. Many sites are clustered together in densely populated areas. If terrorists cause catastrophic chemical releases or explosions at these key facilities, large numbers of Americans will be put at risk of injury or death. Such attacks may also have a devastating impact on the U.S. economy. Surprisingly, in light of these risks most chemical sites have not implemented adequate measures to prevent, mitigate, deter, and/or respond to terrorist attacks. This thesis proposes that private and public sectors partner together to improve the preparedness of chemical facilities for acts of terrorism. More specifically, key stakeholders from both sectors need to forge Regional Defense Units (RDUs). Their primary purpose is to effectively reduce the attractiveness of regional chemical facilities as targets for terrorists. To achieve this goal, a mixture of mandates (sticks) and incentives (carrots) need to be regionally developed, implemented, and sustained by RDUs. Collaborative regional efforts using an appropriately balanced and community-governed carrot and stick approach

can be the most effective option for federal policymakers and the Department of Homeland Security to improve chemical facility preparedness, and thus homeland security.

0590 **Baldauf, Paul D., *Chemical Industry Security: Voluntary or Mandatory Approach*, Naval Postgraduate School, March 2007. 93pp.**

A successful attack on a hazardous materials storage facility has the potential to cause mass casualties and panic. Although the risk and consequences vary greatly among these sites, there are a significant number of facilities with tens of thousands of individuals who live and work in the vulnerability zone. Until P.L. 109-125 was enacted on October 4, 2006, which required the Department of Homeland Security (DHS) to issue regulations establishing risk based performance standards, the Federal government policy for securing chemical facilities from terrorist attack relied entirely upon voluntary actions by industry. Though it is sure to create controversy, this thesis proposes the need for new legislation that mandates standards for chemical industry security yet also addresses the economic and implementation impacts. DHS, in close partnership with the Environmental Protection Agency (EPA), is best suited to undertake this responsibility. In addition, State delegation of oversight responsibility is necessary to address the resources required to handle such a large number of sites. Public participation in preparedness and response activities is vital to reduce the fear and anxiety inherent to acts of terrorism. Inherently Safer Technology evaluations are recommended for the chemical sector through regulatory amendments to the Clean Air Act Section 112.

0682 **Persily, Andrew, et al., *Building Retrofits for Increased Protection Against Airborne Chemical and Biological Releases,* National Homeland Security Research Center, Environmental Protection Agency, March 2007. 178pp.**
Due to concerns about potential airborne chemical and biological (chembio) releases in or near buildings, building owners and managers and other decision makers are considering retrofitting buildings to provide some degree of protection against such events. A wide range of technologies and approaches are being proposed with varying levels of efficacy and cost, as well as varying degrees of applicability to particular buildings and ventilation systems. This document presents the results of an effort to evaluate chembio retrofit options for buildings. A number of retrofit options are identified, and their potential to protect building occupants from a number of generic contaminant releases is evaluated using building airflow and contaminant transport modeling. In addition, a case study is presented in which specific retrofit options were considered for two actual buildings and pre-installation designs and cost estimates were developed.

0860 **Kesavan, Jana S., *Characteristics and Sampling Efficiencies of Portable High Throughput Liquid-Assisted Aerosol Sampler Model APAS-2,* Edgewood Chemical Biological Center, April 2007. 17pp.**

Characteristics and aerosol sampling efficiencies of a Portable High Throughput Liquid-Assisted Air Sampler Model APAS-2 (PHTLAAS-APAS-2) (Zaromb Research Corp., Hinsdale, IL) were determined at the U.S. Army Edgewood Chemical Biological Center (ECBC). The PHTLAAS-APAS-2 is a portable, battery-operated bioaerosol sampler designed to collect 0.5- to 10-micrometers particles into a buffer solution to preserve the viability of bio-organisms.

0877 **Denlinger, Rebecca F.,** ***National Infrastructure Advisory Council, Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce: Final Report and Recommendations,*** **National Infrastructure Advisory Council, January 8, 2008. 89pp.**

The National Infrastructure Advisory Council (NIAC) convened a Working Group to study the impact of chemical, biological, and radiological (CBR) events on the critical infrastructure worker, and to make recommendations. NIAC designed this report to identify attributes of different chemical, biological, or radiological event scenarios, identify key elements necessary to sustain critical infrastructure operations, and to make recommendations that will improve our ability to contain the impact, recover from its consequences, and restore the nation's critical infrastructure to a pre-event state. The Executive Summary highlights key themes found throughout the document, and identifies a number of findings and recommendations that are common across CBR events. Included in subsequent sections are appendices that identify specific findings and recommendations unique to chemical, biological, or radiological events.

0966 **U.S. Joint Chiefs of Staff,** ***Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments,*** **U.S. Joint Chiefs of Staff, August 26, 2008. 147pp.**

This publication provides doctrine to assist commanders and staffs in planning, preparing for, conducting, and assessing operations in which their forces may encounter chemical, biological, radiological, and nuclear threats and hazards. These principles apply across the range of military operations. It has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces in joint operations and provides the doctrinal basis for interagency coordination and for US military involvement in multinational operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations, education, and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall objective.

REEL 17

Chemical Terrorism cont.

0001 **Kosal, Margaret E.,** ***Chemical Terrorism: U.S. Policies to Reduce the Chemical Terror Threat,*** **Partnership for a Secure America, September 2008. 31pp.**

This study recognizes significant US government progress in detecting and mitigating chemical terror threats, including enhancements in interagency coordination. It finds similarly noteworthy progress in elimination of military chemical stockpiles, though the pace could be faster and much remains to be done. Challenges remain, however, in the need for stronger multilateral cooperation to prevent proliferation, and for a more serious and comprehensive effort to secure chemical facilities and transportation infrastructure against theft or attack.

0032 **Orum, Paul, *Chemical Security 101: What You Don't Have, Can't Leakm or Be Blown Up by Terrorists*, Center for American Progress, November 2008. 55pp.**

This report finds that most of the nation's 101 most dangerous chemical facilities could switch to safer, more secure chemicals or processes. Making these changes would significantly reduce or eliminate the threat to 80 million Americans living near these facilities and millions more living along train or truck delivery routes.

Cyberterrorism

0087 **Presby, Timothy D., *Computer Network Attack and Its Effectiveness Against Non-State Actors*, Naval War College, February 13, 2006. 23pp.**

Computer Network Attack (CNA) is a subset of Computer Network Operations (CNO), which is a core capability of Information Operations. CNA is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. With the United States engaged in counter-insurgency operations against terrorist groups, synchronizing the effects of CNA with more traditional forms of kinetic attacks, as well as other instruments of national power, permits the United States to achieve its political and military objectives at a reduced cost. The dependency of non-state adversaries on computer systems will only grow as information systems become more pervasive in under-developed nations. CNA, while typically not decisive in itself, can help shape the battle space and serve as an effective instrument against non-state actors.

0110 **Barwinski, Mark, et al., *Empirical Study of Drive-by-Download Spyware*, Naval Postgraduate School, March 2006. 13pp.**

The ability of spyware to circumvent common security practices, surreptitiously exporting confidential information to remote parties and illicitly consuming system resources, is a rising security concern in government, corporate, and home computing environments. While it is the common perception that spyware infection is the result of high risk Internet surfing behavior, our research shows main-stream web sites listed in popular search engines contribute to spyware infection irrespective of patch levels and despite "safe" Internet surfing practices. Experiments conducted in July of 2005 revealed the presence of spyware in several main-stream Internet sectors as evidenced in the considerable infection of both patched and unpatched Windows XP test beds. Although the experiment emulated conservative web surfing practices by not interacting with web page links, images, or banner advertisements, spyware infection of Internet Explorer based test beds occurred swiftly through cross-domain scripting and ActiveX exploits. As many as 71 different spyware programs were identified among 6 Internet sectors. Real estate and online travel-related web sites infected the test beds with, as many as 14 different spyware programs and one bank-related web site appeared to be the source of a resource consuming dialing program. Empirical analysis suggests that spyware infection via drive-by-download attacks has thus far been unabated by security patches or even prudent web surfing behavior. At least for the moment, it appears the choice of web browser applications is the single most effective measure in preventing spyware infection via drive-by-downloads.

0123 **Ye, Nong, *Automatic Extraction and Coordination of Audit Data and Features for Intrusion and Damage Assessment,* AFOSR, March 31, 2006. 94pp.**

Intrusion and damage assessment is an important step after intrusion detection. The goal of this research is to shorten time of constructing a coherent intrusion trace and assessing the damage through automatic extraction and coordination of audit data and features for intrusion and damage assessment. In this project, we develop the System- Fault-Risk framework to define cause-effect chains of intrusions as intrusion profiles and also classify intrusions. We create a new attack-norm separation approach to developing detection models for building cyber sensors monitoring and identifying intrusion data characteristics at various points along the path of an intrusion cause-effect chain. Mean, autocorrelation and wavelet data characteristics of cyber attack and norm data are discovered to enable the definition of attack data models and norm data models which are in turn used to build detection models for cyber sensors. The testing results the superior performance of detection models based on the attack-norm separation approach to that of detection models based on two conventional approaches of signature recognition and anomaly detection.

0217 **Interagency Working Group on Cyber Security and Information Assurance, *Federal Plan for Cyber Security and Information Assurance Research and Development,* National Science and Technology Council, April 2006. 133pp.**

In today's environment of heightened risk, the Federal government has an essential role to play in cyber security and information assurance (CSIA) research and development (R&D). As in other science, technology, and engineering fields of critical importance to the Nation, Federal leadership should energize a broad collaboration with private-sector partners and stakeholders in academia and the national and industry laboratories where the bulk of Federal research is carried out. Such a partnership can chart a national R&D agenda for strengthening the security of the Nation's IT infrastructure. This Federal Plan for Cyber Security and Information Assurance Research and Development takes the first step toward developing that agenda. The Plan also responds to recent calls for improved Federal cyber security and information assurance R&D, as outlined in the following documents: the OSTP/OMB Memorandum on Administration FY 2007 R&D Budget Priorities; Cyber Security: A Crisis of Prioritization, the 2005 report of the President's Information Technology Advisory Committee (PITAC); the 2003 National Strategy to Secure Cyberspace; and the 2002 Cyber Security Research and Development Act (P.L. 107-305). Developed by the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), an organization under the National Science and Technology Council (NSTC), the Plan provides baseline information and a technical framework for coordinated multiagency R&D in cyber security and information assurance.

0351 **Cumiford, Leslie D., *Situation Awareness for Cyber Defense,* Sandia National Laboratories, June 2006. 28pp.**

Situation awareness (SA), or the ability to assess situations and prepare timely responses, has long been acknowledged as an important aspect of theater operations for defensive purposes. Likewise, SA is critical in the cyber world. The focus of this paper is SA in the cyber domain with respect to defensive capabilities. The cyber defense domain has an important characteristic in common with related domains such as analysis of terrorism, protection of infrastructure, and IED defense: the domains are characterized by sets of complex,

interacting issues that are ill-defined, ambiguous, and evolving in time. Solutions for such problems must be integrative, handle domain complexity, and incorporate and address the element of surprise. A list of the capabilities needed to accomplish effective cyber SA is provided, along with an architecture for cyber SA reasoning. Most cyber SA architectures attempt to mirror the complexity of the domain. Surprisingly, the latest brain research does not support this approach. Notional information is provided regarding a new approach to cyber situation awareness, taking into account the lessons learned from the way humans process such information.

0380 **Denning, Dorothy E., *A View of Cyberterrorism Five Years Later*, Naval Postgraduate School, [no month] 2006. 19pp.**

The purpose of this report is to assess the cyberterror threat, particularly from al-Qa'ida and the global jihadists who are part of the broader social movement associated with al-Qa'ida. As such, the view offered here supercedes that which the author presented 5 years ago, first to the Special Oversight Panel on Terrorism of the Committee on Armed Services in the U.S. House of Representatives in May 2000, and then in an article written shortly after the September 11 attacks in 2001. This assessment was based primarily on speculation as to what terrorists would likely be interested in and capable of achieving. The author's overall conclusion was that, at least for the time being, bombs posed a much greater threat than bytes, but the United States should not shrug off the threat. The assessment offered in this paper is based less on speculation and more on indicators of cyberterrorism.

0399 **Tester, Rodrick A., *Risk of Cyberterrorism to Naval Ships In-Port, Naval Station Everett: A Model Based Project Utilizing SIAM*, Naval Postgraduate School, March 2007. 94pp.**

Based on numerous high level concerns that the cyber threat is expected to increase, as well as the already documented uses of cyber warfare, it is necessary to ensure our naval ships are hardened against such attacks. In doing so, an influence net model was designed to discover the likelihood of a successful cyber attack However, first it was necessary to establish what the best mitigation tools are in defense of cyber attack methods. In order to do so, an expert opinion survey was designed and completed by individuals currently working in the field of network security. In combination with the expert opinion surveys and in looking at research and established security techniques it should become apparent whether or not ships are taking all the required steps to best secure themselves against an attack. Though the initial model was designed around a theoretical Naval Station Everett ship, with modification the model can be utilized for any naval asset throughout the United States and the risk for each particular U.S. asset can be evaluated. Additionally, this tool can also facilitate security funding as well as establishing a means of prioritizing the tools for protection if the network needs to be hastily re-established after an attack. Ultimately, the protection of a ship's computer networks against cyber terrorist threats is fundamental in ensuring continued effective command and control and ultimately the security of this nation.

0493 **Park, Joon, *Dynamic Hybrid Component Test for Mission-Critical Distributed Systems*, Air Force Research Laboratory, Rome, NY, June 2007. 28pp.**

The objective of this effort was to provide dynamic and hybrid survivability mechanisms that test a downloaded component in runtime in the current computing environment by

considering N-category, N-type, and N-way testing methods. The test results can be used to fix the failures or immunize the component based on our previous research outcomes.

0521 **Kruger, Martin, *Game Theoretic Solutions to Cyber Attack and Network Defense Problems,* Office of Naval Research, June 2007. 37pp.**

There are increasing needs for research in the area of cyber situational awareness. The protection and defense against cyber attacks to computer network is becoming inadequate as the hacker knowledge sophisticates and as the network and each computer system become more complex. Current methods for alert correlation to detect and identify network attacks rely on data mining approaches that use features or feature sets of network data to discover an attack. These approaches are useful for simple attacks but for complex or coordinated cyber intrusions, they have various issues such as false positive, limited scalability, limits on detecting new types of coordinated and sophisticated cyber attacks. Therefore, the cyberspace security requires next-generation network management and intrusion detection systems that combine both short-term sensor information and long-term knowledge databases to provide decision-support systems and cyberspace command and control. In this paper, we propose a game theoretic high level information fusion based decision and control framework to detect and predict the multistage stealthy cyber attacks. The main focus of this paper is to address the cyber network security problem from a system control and decision perspective and revise the Markov game model with the knowledge of the cyber attack domain.

0559 **Courville, Shane P., *Air Force and the Cyberspace Mission Defending the Air Force's Computer Network in the Future,* Air War College, December 2007. 58pp.**

This paper recommends that the Air Force pursue research in quantum encryption and security, and continue to examine computer security techniques for the mid-term and beyond. The Air Force should continue future planning efforts to anticipate and develop countermeasures to emerging threats in order to proactively protect and dominate the cyberspace domain of the future. This paper argues that America's future adversaries can, and will, use information technology as a means to wage warfare in the cyberspace domain against the United States. The Air Force is highly dependent on computers and information operations, and will be even more dependent in the next 20 years. The majority of computers, their operating systems, and software purchased by the Air Force are commercial off-the-shelf (COTS) components, often manufactured abroad due to cheaper cost. Thus, foreign countries could place hidden components inside the computers, making the computers vulnerable for attack and/or spying. Furthermore, Air Force networks are connected to and utilize the internet, which also is vulnerable for exploitation.

0618 **DiBiasi, Jeffrey R., *Cyberterrorism: Cyber Prevention vs. Cyber Recovery,* Naval Postgraduate School, December 2007. 65pp.**

The technological age has forced the U.S. to engage a new set of national security challenges. Several potential adversaries have cyberspace capabilities comparable to those of the U.S., and are constantly conducting surveillance, gathering technical information, and mapping critical nodes that could be exploited in future conflicts. Recent policy documents set out a strategy for securing all of cyberspace, which experts argue is impossible to implement, but also unnecessary. This thesis seeks to move the discussion beyond this stalemate by

undertaking an analysis of the vulnerability of cyberspace to terrorist attacks. The first analysis examines the Code Red Worm and the Slammer Worm. These two worms were selected because they were highly destructive and spread faster than normal worms, making them well suited for assessing the existing security of computers and networks. The next analysis examines a staged cyber attack on critical infrastructure, entitled Attack Aurora. In the staged Aurora attack, researchers from the Department of Energy's Idaho lab hacked into a replica of a power plant's control system. This attack is the most recent staged attack and facilitates an analysis of vulnerabilities of critical infrastructures to cyberterrorism.

0682 **McQueen, Miles, et al., *Measurable Control System Security through Ideal Driven Technical Metrics*, Idaho National Laboratory, January 2008. 26pp.**

The Department of Homeland Security National Cyber Security Division supported development of a small set of security ideals as a framework to establish measurable control systems security. Based on these ideals, a draft set of proposed technical metrics was developed to allow control systems owner-operators to track improvements or degradations in their individual control systems security posture. The technical metrics development effort included review and evaluation of over thirty metrics-related documents. On the bases of complexity, ambiguity, or misleading and distorting effects the metrics identified during the reviews were determined to be weaker than necessary to aid defense against the myriad threats posed by cyber-terrorism to human safety, as well as to economic prosperity. Using the results of the metrics review and the set of security ideals as a starting point for metrics development, the assessment identified thirteen potential technical metrics - with at least one metric supporting each ideal.

0708 **Wilson, Clay, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service, Library of Congress, January 29, 2008. 43pp.**

Cybercrime is becoming more organized and established as a transnational business. High technology online skills are now available for rent to a variety of customers, possibly including nation states, or individuals and groups that could secretly represent terrorist groups. The increased use of automated attack tools by cybercriminals has overwhelmed some current methodologies used for tracking Internet cyberattacks, and vulnerabilities of the U.S. critical infrastructure, which are acknowledged openly in publications, could possibly attract cyberattacks to extort money, or damage the U.S. economy to affect national security.

0751 **Kelley, Olen L., *Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative*, U.S. Army War College, March 15, 2008. 32pp.**

In 2001, Joint Publication (JP) 3-0 identified five warfighting domains. The document contained the commonly accepted four operational environments, but added a new domain: "information." This landmark inclusion started an intense debate within the Joint community. Previous clarity on the commonly accepted operational environment's roles and functions became blurred. Those who advocated information as a warfighting domain advanced its common understanding, yet could not reach doctrinal consensus. Discussions about how to describe, organize, and use the United States' information capabilities to support the Department of Defense's (DoD) strategic and operational objectives and national security goals remain contentious and ambiguous. This inability to develop consensus led to the re-

characterization of information in the current JP 3-0, "Joint Operations," from a warfighting domain to an "environment." However, this change did not resolve the fundamental issue and the information domain debate continues unabated. The recently published "National Military Strategy for Cyberspace Operations" (NMS-CO) again officially codified its understanding of "information," now defined as cyberspace, as a warfighting domain. It acknowledges the JP 3-0 information domain change to environment, but emphasizes that "treating cyberspace as a domain establishes a foundation to understand and define its place in military operations." The DoD has expended considerable effort in a "piece meal" strategy that updates information-related doctrine based on new technology instead of developing a comprehensive cyberspace strategy. This paper argues that a clear consensus is needed to establish a "cyberspace domain" where JFCs conduct war "as an act of force to compel our enemy to do our will." Advancing the proposed NMS-CO's cyberspace domain definition clarifies information operation's roles and functions, thereby enabling information superiority.

0783 **Skarda, Bryan, et al.,** ***C2 for Complex Endeavors: Operationalizing Social Engineering for Offensive Cyber Operations,*** **U.S. Air Force Institute of Technology, June 2008. 14pp.**

Social Engineering describes a class of computer hacking that targets the user of the system rather than the hardware or software. It is a proven and viable vector that includes techniques like phishing, pharming, and persuasion. The Air Force uses social engineering to a limited extent as a validation tool when assessing the security stance of a unit or installation. Units like the 57th Information Aggressor Squadron based at Nellis Air Force Base routinely employ social engineering techniques as they perform their mission. However, this is the only employment of social engineering currently evidenced in the Air Force inventory. Based on the widespread success of these techniques in the civilian world, anecdotal evidence gleaned from both interviews and literature reviews places their effectiveness at or near 100 percent, social engineering seems a logical fit for an organization looking for the next best weapon. Additionally, social engineering has the rare and enviable trait of being extremely low cost, both in terms of training and execution. These factors inspired this research along with the perceived lack of interest given the topic inside the Air Force. Further investigation into social engineering evidenced little academic attention devoted to the topic which seemed disproportionate to the technique's reported level of effectiveness. With the material presented here, the aim is to demonstrate that social engineering as a concept already exists in current doctrine and that, with a little adaptation, a widely practiced methodology exists that can be used to structure social engineering attacks and evaluation.

0797 **Rowe, Neil C.,** ***C2 for Complex Endeavors: Automatically Tracing Information Flow of Vulnerability and Cyber-Attack Information through Text Strings,*** **U.S. Air Force Institute of Technology, June 2008. 43pp.**

Quick dissemination of information about new vulnerabilities and attacks is essential to time-critical handling of threats in information security, but little systematic tracking has been done of it. We are developing data mining techniques to track the flow of such information by comparing important information-security Web sites, alert messages, and strings in packets to find similar words and sentences. We report on tools we have developed to collect relevant sentences, with a particular focus on comparing sentences from different sources to find patterns of quotation and influence. We report results on some representative pages that indicate some surprising information flows, for which the combination of both word

matching and structure matching performed significantly better than either alone. We also report on preliminary work on the front lines of cyber-attack, trying to correlate text in intrusion-detection reports and even attack packets observed on a honeypot with reports of known attacks. These methods could help us automatically locate relevant fixes quickly when being attacked. Our tools will in general enable better design of incident response and incident reporting requirements for organizations, by showing bottlenecks and unused capabilities in the management of vulnerabilities and attacks.

0841 **Grimalia, Michael R.,** ***C2 for Complex Endeavors: An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mission Impact Assessment,*** **U.S. Air Force Institute of Technology, June 2008. 53pp.**

The use of information technologies to enhance Command and Control (C2) processes has yielded enormous benefits in military operations. Commanders are able to make higher quality decisions by accessing multiple information resources; obtaining frequent updates; and by correlation between resources to reduce battlespace uncertainty. However, the dependence upon information technology creates significant operational risk that is often overlooked and is frequently underestimated. Risk management is the accepted process used to identify, value, and protect critical assets commensurate with their value. Risk analysis, the first step of the risk management process, requires the identification and documentation of organizational resources and determination of their criticality. While risk analysis is conceptually easy to understand, in practice it is difficult to conduct due to the dynamic nature of organizations, the temporal nature of operations, and the inherent subjectivity associated with valuation. This paper proposes a scalable, self-documenting, distributed information asset tracking methodology that identifies information dependencies, does not incur significant overhead, and prevents an adversary gaining knowledge from intercepted communications. The method is made feasible via the wide-spread deployment of Host-Based System Security software agents by JTF-GNO and can significantly enhance cyber damage assessment timeliness and accuracy and enables mission impact assessment.

0895 **Cosnowski, Charles R.,** ***Defeating 802.11 Wireless Networks,*** **U.S. Air Force Institute of Technology, June 2008. 56pp.**

Homeland Security of the United States is constantly under threat of attack from terrorist organizations. A variable and current terrorist threat is the use of unmanned aerial vehicles (UAVs) as weapons of mass destruction. These UAVs can be built simply and cheaply from commercial off the shelf (COTS) parts and are typically controlled using standard radio control (RC) technology. An emerging technology that is being implemented to control and communicate with UAVs is the 802.11 wireless network protocol or Wi-Fi. This project discusses various portions of the Wi-Fi protocol and analyzes the protocol to determine techniques for first detecting and then defeating wireless networks utilizing the protocol through denial or deception. The first set of techniques presented defeats a network through denial. These denial techniques are divided into two categories: broad area denial techniques and specific network denial techniques. After denial techniques are discussed a process for deceiving an 802.11 wireless network is presented.

0951 **Hunsberger, Michael G., *A Methodology for Cybercraft Requirement Definition and Initial System Design*, U.S. Air Force Institute of Technology, June 2008. 178pp.**

The United States Air Force and Department of Defense networks and information systems are under attack from a variety of actors. Current network defense systems are reactive in nature and unable to prevent determined adversaries from successfully infiltrating these information systems. The realization of these facts led the Air Force Research Lab begin work on a next-generation network defense system called Cybercraft. The Cybercraft vision is a trusted, autonomous system which will perform network defense tasks. In this paper, software engineering and threat analysis are used to create a set of initial requirements and system models for Cybercraft. This paper presents a methodology based on traditional software requirements, elicitation processes, and attack and defense trees to generate system requirements. Once requirements have been defined, they are used to create system use cases and a system domain model. This iterative process can be used to define the system in enough detail that software or system prototypes can be developed. The contribution of this paper is a set of initial requirements, use cases, and domain models which could be used in Cybercraft development. Ultimately, it is a generic methodology which could be used to determine requirements for any security system and how to apply those requirements to begin high-level system design.

REEL 18

Infrastructure Protection and Security

0001 **Durling, R.L., Jr., and D.E. Price, *Use of Homeland-Defense Operational Planning System (HOPS) for Emergency Management*, Lawrence Livermore National Laboratory, January 5, 2006. 9pp.**

For over ten years, the Counter-proliferation Analysis and Planning System (CAPS) at Lawrence Livermore National Laboratory (LLNL) has been a planning tool used by U.S. combatant commands for mission support planning against foreign programs engaged in the manufacture of weapons of mass destruction (WMD). The Homeland-Defense Operational Planning System (HOPS) is a new operational planning tool leveraging CAPS expertise designed to support the defense of the U.S. homeland. HOPS provides planners with a basis to make decisions to protect against acts of terrorism, focusing on the defense of facilities critical to U.S. infrastructure. Criticality of facilities, structures, and systems is evaluated on a composite matrix of specific projected casualty, economic, and sociopolitical impact bins. Based on these criteria, significant unidentified vulnerabilities are identified and secured.

0010 **Jaksec, Gregory M.,** ***Public-Private-Defense Partnering in Critical Infrastructure Protection,*** **Naval Postgraduate School, March 2006. 60pp.**

The problem confronting The Department of Homeland Security (DHS), the Department of Defense (DoD), and America's private sector is how to collectively protect the nation s critical infrastructure. The challenge for the DHS is in motivating partnerships across the public, private, and DoD domains, each with different organizational and cultural objectives governed under a federalist system. The relevance of this problem lies in the vulnerability of America s economic and military foundations to terrorist attacks or a catastrophic natural disaster. Research conducted of the regulated energy and water industries indicates federal standards can be effectively established across the public-private domains. The establishment of federal tax and insurance incentives, limiting corporate liability, and developing industry standards may motivate increased security and circumvent excessive federal mandates. The conduct of partnering is scrutinized via personal interviews to determine if the recommendation to build security partnerships with federal guidance is sufficient to secure critical infrastructure. The implementation of a dual-purpose strategy is recommended to further enhance the efficiency of security partnerships. This thesis suggests the DHS must develop an innovative CIP policy and utilize the National Infrastructure Protection Plan (NIPP) as the vehicle to integrate and synchronize the actions of all security partners.

0070 **Santiago, Denise L.,** ***Assessment of Public Health Infrastructure to Determine Public Health Preparedness,*** **Naval Postgraduate School, March 2006. 104pp.**

Since September 2001, health threats associated with acts of terrorism have become an area of increasing concern. The Strategy for Homeland Security stresses the need for a robust public health component to quickly respond to and recover from attacks and other emergencies. The assumption that public health is an optimal system that simply needs to be aimed in new directions is fundamentally flawed. Public health baseline requirements for responding to threats are not as well understood as they might be. The purpose of this research is to help establish a common and accurate measure for assessing the public health infrastructure. Using the case study of Union County, New Jersey this thesis surveys the activities public health agencies are expected to perform; compares performance to target objectives; and employs a manpower matrix as a model for determining staffing requirements for local public health. This study argues that that the goal of sustainable funding for public health begins with an accurate measure of the capacities of the system in relation to demands placed upon it. Without such a measure public health will continue to fail in its primary functions and lack the capacity to meet Homeland Security goals.

0174 **Martin, Christopher,** ***Protecting America's Critical Infrastructure: Making Our Program More Effective,*** **U.S. Army War College, March 15, 2006. 28pp.**

Critical Infrastructure in the United States is defined by the Patriot Act of 2001 as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” The United States is challenged to protect its critical infrastructure from attacks by terrorists and from natural disasters for a variety of reasons. A contributing reason for inefficiencies is the way the current program as established by Homeland Security Presidential Directive 7 (HSPD-7) (2003) assigns responsibilities. The author addresses the definition of critical

infrastructure and attempts to determine if this definition is adequate, and then moves to an examination of the current program to see if there are ways to gain efficiencies and effectiveness. In addition, he determines if there is a common method to analyze critical infrastructure (i.e., vulnerability, risk, and cost-benefit analysis) to determine how the United States should prioritize funding for critical infrastructure protection. Finally, recommendations are provided to make the critical infrastructure program more effective.

0202 **Moteff, John D., *Critical Infrastructures: Background, Policy, and Implementation,* Congressional Research Service, Library of Congress, April 18, 2006. 36pp.**

The nation's health, wealth, and security rely on the production and distribution of certain goods and services. The array of physical assets, functions, and systems across which these goods and services move are called critical infrastructures. The national security community has been concerned for some time about the vulnerability of critical infrastructure to both physical and cyber attack. Given the physical damage caused by the September 11 attacks, physical protection of critical infrastructures has received increased attention. Following the events of September 11, the Bush Administration released Executive Order 13228, signed October 8, 2001, establishing the Office of Homeland Security and the Homeland Security Council. Among its responsibilities is overall coordination of critical infrastructure protection activities. In June 2006, the Bush Administration released a National Infrastructure Protection Plan.

0238 **Government Accountability Office, *Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts,* U.S. Government Accountability Office, May 2006. 71pp.**

The need to better protect federal facilities, coupled with federal budget constraints and the increased scrutiny of homeland security funding and programs, has prompted the need for U.S. agencies to measure the performance of their facility protection efforts. In this environment, it is important for these agencies to ensure that investments in facility protection are providing adequate returns in terms of better protecting real property assets against terrorism. In addition, the U.S. government's national strategy, Presidential directive, and guidance on protecting critical infrastructures--including facilities--have identified the use of performance measurement as a key means of assessing the effectiveness of protection programs. Given that protection of critical infrastructures is an important issue for organizations outside of the federal government as well, it is beneficial to look to the experiences of these organizations to identify lessons learned.

0311 **Federal Emergency Management Agency, *Safe Rooms and Shelters: Protecting People against Terrorist Attacks,* Federal Emergency Management Agency, May 2006. 262pp.**

The objective of this manual is to provide guidance for engineers, architects, building officials, and property owners to design shelters and safe rooms in buildings. This manual presents information about the design and construction of shelters in the work place, home, or community building that will provide protection in response to manmade hazards.

0573 **Council of State Governments, *The Impact of Terrorism on State Law Enforcement: Adjusting to New Roles and Changing Conditions,* National Institute of Justice, June 2006. 96pp.**

The catastrophic events of Sept. 11, 2001, served as a wake-up call to the nation regarding the threat of terrorism. Preventing future acts of terrorism and preparing for massive response operations became a national priority overnight for law enforcement at all levels, creating new responsibilities and new paradigms for federal, state and local law enforcement agencies. In 2003, The Council of State Governments and Eastern Kentucky University set out to explore these new roles and changing conditions. Among other components of this 18-month effort, researchers conducted a 50-state survey of state and local law enforcement agencies, conducted a series of case studies, and convened an expert work group of public officials. According to the survey results, state law enforcement agencies are very involved in their states' homeland security initiatives. Combined with new demands for collaboration with other branches of government and the private sector, state police personnel and resources are stressed.

0669 **Department of Homeland Security, *National Infrastructure Protection Plan*, U.S. Department of Homeland Security, June 2006. 196pp.**

Protecting the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. Attacks on CI/KR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the Nation's CI/KR as weapons of mass destruction could have even more devastating physical and psychological consequences. The overarching goal of the National Infrastructure Protection Plan (NIPP) is as follows: Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency. The NIPP provides the unifying structure for the integration of existing and future CI/KR protection efforts into a single national program to achieve this goal. The NIPP framework will enable the prioritization of protection initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters. The NIPP risk management framework recognizes and builds on existing protective programs and initiatives.

0861 **Larsen, Jeffrey A., and Tasha L. Pravecek, *Comparative U.S.-Israeli Homeland Security,* U.S. Air Force Counterproliferation Center, U.S. Air University, June 2006. 130pp.**

This report examines the premise that there are lessons from Israeli experience that might enhance the United States' homeland security efforts. The research for this study included a literature review and field interviews with American and Israeli leaders in Washington, D.C., and Israel during the summer of 2005. The report addresses the common and unique threats

facing each state and related homeland security issues and policies. It begins with the threats experienced by each nation, examining the respective homeland security organizational structures and ways of preventing attacks and responding to attacks that do occur. The report then compares each country's homeland security program. Where appropriate, personal observations derived from the authors' interviews in each country are included. The final section addresses a series of lessons the United States might consider in its efforts to improve its homeland security, as well as a discussion of where it might not be advantageous or feasible to follow the Israeli model. The United States and Israel each face a number of threats to their homeland -- some shared, some unique to each state. Some threats common to both the United States and Israel include the following: Terrorism and the Global War on Terror, State Aggression by Sovereign Powers, Weapons of Mass Destruction, and Trans-Border Issues. The report discusses the organizational structures that the United States and Israel employ to respond to threats, the countries' efforts at preventing terrorist attacks, and comparative efforts to respond to an attack. The research and field interviews conducted by the authors to identify lessons from Israeli experience resulted in the following recommendations: know your adversary, interagency cooperation, tight internal security, profiling, protected spaces, barriers, information sharing, public education, offensive military action, security decision making, compromise and appeasement, and advanced technology.

0991 **Jones, Dean A., et al.,** ***Physical Security and Vulnerability Modeling for Infrastructure Facilities,*** **Sandia National Laboratories, July 2006. 32pp.**

A model of malicious intrusions in infrastructure facilities is developed, using a network representation of the system structure together with Markov models of intruder progress and strategy. This structure provides an explicit mechanism to estimate the probability of successful breaches of physical security, and to evaluate potential improvements. Simulation is used to analyze varying levels of imperfect information on the part of the intruders in planning their attacks. An example of an intruder attempting to place an explosive device on an airplane at an airport gate illustrates the structure and potential application of the model.

REEL 19

Infrastructure Protection and Security cont.

0001 **Ordonez, Michael A.,** ***Critical Infrastructure Protection: How to Assess and Provide Remedy to Vulnerabilities in Telecom Hotels,*** **Naval Postgraduate School, September 2006. 108pp.**

America's open society includes a vast array of critical infrastructure and key resources that are vulnerable to terrorist attacks. While it is not possible to protect or eliminate vulnerabilities of all critical infrastructures in the United States, strategic improvements can be made to harden these assets and mitigate any damaging effects if an attack were to occur. Current network assessment methods and protective measures are inadequate. As a consequence, the need for a scientific methodology for implementation of critical infrastructure protection is required. A standardized vulnerability assessment/risk analysis tool needs to be developed and implemented for the Critical Infrastructure Protection Programs to analyze complex networks and examine critical nodes. This will help to prevent,

deter, and mitigate the effects against terrorist attack in accordance with HSPD-7. This thesis examines ways in which vulnerability analysis is currently conducted and ways in which it could be improved to establish an all-encompassing methodology to identify, prioritize, and protect critical infrastructure. Based on analysis and research, the thesis recommends that the National Communications System under the Department of Homeland Security (DHS) establish the required policy initiatives to mandate the National Reliability and Interoperability Council's current and future best practices, and set a vulnerability assessment/analysis standard based on Model-Based Vulnerability Analysis (MBVA) and Joint Staff Integrated Vulnerability Assessment (JSIVA) methodologies.

0109 **Wiberg, Kenneth C.,** ***Identifying Supervisory Control and Data Acquisition (SCADA) Systems on a Network via Remote Reconnaissance,*** **Naval Postgraduate School, September 2006. 147pp.**

Presidential Decision Directive (PDD) 63 calls for improving the security of Supervisory Control and Data Acquisition (SCADA) and other control systems which operate the critical infrastructure of the United States. In the past, these industrial computer systems relied on security through obscurity. Recent economic and technical shifts within the controls industry have increased their vulnerability to cyber attack. Concurrently, their value as a target has been recognized by terrorist organizations and competing nation states. Network reconnaissance is a basic tool that allows computer security managers to understand their complex systems. However, existing reconnaissance tools incorporate little or no understanding of control systems. This thesis provided a conceptual analysis for the creation of a SCADA network exploration/reconnaissance tool. Several reconnaissance techniques were research and reviewed in a laboratory environment to determine their utility for SCADA system discovery. Additionally, an application framework using common non-SCADA security tools was created to provide a proof of concept. Development of a viable tool for identifying SCADA systems remotely will help improve critical infrastructure security by improving situational awareness for network managers.

0255 **Government Accountability Office,** ***Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics,*** **U.S. Government Accountability Office, October 2006. 64pp.**

As Hurricane Katrina so forcefully demonstrated, the nation's critical infrastructures and key resources have been vulnerable to a wide variety of threats. Because about 85 percent of the nation's critical infrastructure is owned by the private sector, it is vital that the public and private sectors work together to protect these assets. The Department of Homeland Security (DHS) is responsible for coordinating a national protection strategy including formation of government and private sector councils as a collaborating tool. The councils, among other things, are to identify their most critical assets, assess the risks they face, and identify protective measures, in sector-specific plans that comply with DHS's National Infrastructure Protection Plan (NIPP). GAO examined (1) the extent to which these councils have been established; (2) the key facilitating factors and challenges affecting the formation of the councils; and (3) the overall status of the plans and key facilitating factors and challenges encountered in developing them. GAO obtained information by reviewing key documents and conducting interviews with federal and private sector representatives. GAO is not

making any recommendations at this time since prior recommendations are still being implemented. Continued monitoring will determine whether further recommendations are warranted.

0320 **Tussing, Bert B.,** ***Threats at Our Threshold: Homeland Defense and Homeland Security in the New Century,*** **U.S. Army War College, October 21, 2006. 236pp.**

There is no more compelling issue to the government and people of the United States today than Homeland Security. Likewise, there is no more compelling mission for the military than Homeland Defense. But centuries of relative security for a people protected by two oceans and benevolent neighbors to the north and south have left us culturally ill-prepared for a new and ominous era of transitional terrorism that has brought danger to our door. Since the terrible wake-up call of 9/11, we have tried to overcome cultural malaise with institutional renovations, which has led to the greatest reorganization of government since 1947, a reexamination of the direction and focus of our intelligence community, and a renewed concern for domestic defense that has laid near dormant since the early 19th century. in short order this has led to the development of the Department of Homeland Security, the Homeland Security Council, the United States Northern Command, the Office of the Assistant Secretary of Defense for Homeland Defense, a new Director for National intelligence, the National Counterterrorism Center, two committees devoted to Homeland Security oversight in the United States Senate and House of Representatives, and a host of other institutional adjustments in the federal government. These changes were reflected and complemented by an equal commitment to renewal in our states, territories, and local governments, along with an essential commitment by much of the private sector to become active partners in the protection of the country's infrastructure.

0550 **Maguire, Steven, and Shawn Reese,** ***Department of Homeland Security Grants to State and Local Governments: FY2003 to FY2006,*** **Congressional Research Service, Library of Congress, December 22, 2006. 60pp.**

This report analyzes federal grants to state and local governments that are administered by the Department of Homeland Security (DHS). These grants, which are allocated primarily at the discretion of DHS, are intended to enhance homeland security. This report summarizes seven DHS grant programs the State Homeland Security Grant Program (SHSGP), the Urban Area Security Initiative (UASI), the Law Enforcement Terrorism Prevention Program (LETPP), the Emergency Management Performance Grant Program (EMPG), the Metropolitan Medical Response System (MMRS), the Citizen Corps Program (CCP), and the Critical Infrastructure Protection Program (CIP funded only in FY2003). These seven DHS programs were chosen for analysis because the allocations were made to state and local governments, not to private individuals or entities.

0610 **Government Accountability Office,** ***Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks,*** **U.S. Government Accountability Office, January 2007. 119pp.**

GAO is taking stock of key efforts by the President, Congress, federal agencies, and the 9/11 Commission to strengthen or enhance critical layers of defense in aviation and border security that were directly exploited by the 19 terrorist hijackers. Specifically, the report

discusses how: (1) commercial aviation security has been enhanced; (2) visa-related policies and programs have evolved to help screen out potential terrorists; (3) federal border security initiatives have evolved to reduce the likelihood of terrorists entering the country through legal checkpoints; and (4) the Department of Homeland Security (DHS) and other agencies are addressing several major post-9/11 strategic challenges. The report reflects conclusions and recommendations from a body of work issued before and after 9/11 by GAO, the Inspectors General of DHS, State, and Justice, the 9/11 Commission, and others. It is not a comprehensive assessment of all federal initiatives taken or planned in response to 9/11. GAO is not making any new recommendations at this time since over 75 prior recommendations on aviation security, the Visa Waiver Program, and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT), among others, are in the process of being implemented. Continued monitoring by GAO will determine whether further recommendations are warranted.

0729 **Parfomak, Paul W.,** ***Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options,*** **Congressional Research Service, Library of Congress, January 26, 2007. 24pp**.

Critical infrastructure consists of systems and assets so vital to the United States that their incapacity would harm the nation's physical security, economic security, or public health. Critical infrastructure is often geographically concentrated, so it may be distinctly vulnerable to events like natural disasters, epidemics, and certain kinds of terrorist attacks. Disruption of concentrated infrastructure could have greatly disproportionate effects, with costs potentially running into billions of dollars and spreading far beyond the immediate area of disturbance. As the nation's response to recent hurricanes and other disasters continues, and as its homeland security activities evolve, Congress is examining federal policies affecting the geographic concentration and vulnerability of critical infrastructure, including prescriptive siting, economic incentives, environmental regulation, and economic regulation.

0754 **Weiderhold, Fred E.,** ***Rail and Mass Transit Security: Industry and Labor Perspectives,*** **AMTRAK, Office of Inspector General, February 13, 2007. 8pp.**

The challenges to secure Amtrak and make passenger railroading safer from potential terrorists' attacks are daunting. Amtrak operates in 44 states serving over 500 cities and towns across the nation. The nation's rail system is one of the more open, and some say porous, passenger transportation systems in the world, both with respect to physical infrastructure and the very nature of the business itself. Amtrak's stations and trains are, by design, intended to allow persons to move freely unto and off its trains and through its station portals. There are multiple access points throughout our system and it is difficult to fence, gate, and lock down many parts of the system. However, even given these challenges, effective access control and monitoring at critical nodes and around high value assets must be designed and implemented. Any attempt to replicate a TSA-style aviation security architecture would most likely be extremely cost-prohibitive and ineffective. This does not mean that there are not significant lessons to be learned from TSA's aviation security model, and certainly some technologies and monitoring processes to be shared, but the final solution set for passenger rail security must be tailored to its unique environment.

0762 **Government Accountability Office, *Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts,* U.S. Government Accountability Office, March 7, 2007. 25pp.**

The four rail attacks in Europe and Asia since 2004, including the most recent in India, highlight the vulnerability of passenger rail and other surface transportation systems to terrorist attack and demonstrate the need for greater focus on securing these systems. This testimony is based primarily on GAO's September 2005 passenger rail security report and selected recent program updates. Specifically, it addressees (1) the extent to which the Department of Homeland Security (DHS) has assessed the risks facing the U.S. passenger rail system and developed a strategy based on risk assessments for securing all modes of transportation, including passenger rail, and (2) the actions that federal agencies have taken to enhance the security of the U.S. passenger rail system.

0787 **Government Accountability Office, *Critical Infrastructure: Challenges Remain in Protecting Key Sectors,* U.S. Government Accountability Office, March 20, 2007. 28pp.**

This testimony is based primarily on GAO's October 2006 sector council report and a body of work on cyber critical infrastructure protection. Specifically, it addresses (1) the extent to which these councils have been established, (2) key facilitating factors and challenges affecting the formation of the council, (3) key facilitating factors and challenges encountered in developing sector plans, and (4) the status of DHS's efforts to fulfill key cybersecurity responsibilities. GAO has made previous recommendations, particularly in the area of cybersecurity that have not been fully implemented. Continued monitoring will determine whether further recommendations are warranted.

0815 **Nerad, Anton H., II, *Distributed Generation to Counter Grid Vulnerability,* U.S. Army War College, March 30, 2007. 19pp.**

This paper examines how the U.S. can best defend against the interruption of critical electrical energy by hostile acts, identifies and examines some of the vulnerabilities to our nation's power generation and distribution capabilities, outlines several terrorist designs for disruption to it and the resulting economic impact, and provides a possible solution with the adoption of a concept of "distributed generation." It further demonstrates a national recognition of those vulnerabilities and explains who has been assigned the responsibility to protect these capabilities. By providing examples of terrorist targets and highlighting several vulnerabilities, the paper elaborates on the benefits of distributing U.S. energy generation resources and discusses the technologies and their availability, risks, and benefits. Lastly, a discussion concerning ways the government can contribute to the distributed energy picture along with several of the means to best implement and expedite this strategy is provided.

0834 **Department of Homeland Security, *Communications: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan,* U.S. Department of Homeland Security, May 2007. 132pp.**

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of critical infrastructures and key resources (CI/KR) protection efforts into a single National program. The NIPP provides an overall framework for integrating programs and activities that are under way in the various sectors, as well as new and developing CI/KR

protection efforts. The NIPP includes 17 Sector-Specific Plans (SSPs) that detail the application of the overall risk management framework to each specific sector. The Communications SSP describes a collaborative effort among the private sector, Federal Government, and State governments to protect the Nation's Communications Infrastructure. This collaboration will result in the assessment of risk to the communications architecture and its functions that will help prioritize protection initiatives and investments within the sector and aid the identification of critical assets against specific threats.

0961 **Department of Homeland Security*, Water: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan,* U.S. Department of Homeland Security, May 2007. 129pp.**

There are approximately 160,000 public drinking water utilities and more than 16,000 wastewater utilities in the United States. About 84 percent of the U.S. population receives its potable water from these drinking water utilities and more than 75 percent has its sanitary sewage treated by these wastewater utilities. The drinking water and wastewater sector (Water Sector) is vulnerable to a variety of attacks, including contamination with deadly agents and physical and cyber attacks. If these attacks were to occur, the result could be large numbers of illnesses or casualties or denial of service that would also affect public health and economic vitality. Critical services such as firefighting and health care (hospitals), and other dependent and interdependent sectors such as energy, transportation, and food and agriculture, would suffer negative impacts from a denial of Water Sector service. In collaboration with the entire sector, a broad-based strategy to address security needs is being implemented. This work includes providing support to utilities by preparing vulnerability assessment and emergency response tools, providing technical and financial assistance, and exchanging information. Each section of the Water Sector-Specific Plan (SSP), as defined by the Department of Homeland Security (DHS) in its 2006 Sector-Specific Plan Guidance, is described.

REEL 20

Infrastructure Protection and Security cont.

0001 **Government Accountability Office*, Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base,* U.S. Government Accountability Office, August 2007. 41pp.**

The U.S. military relies on the defense industrial base (DIB) to meet requirements to fulfill the National Military Strategy. The potential destruction, incapacitation, or exploitation of critical DIB assets by attack, crime, technological failure, natural disaster, or man-made catastrophe could jeopardize the success of U.S. military operations. GAO was asked to review the Department of Defense's (DOD) Defense Critical Infrastructure Program and has already reported that DOD has not developed a comprehensive management plan for its implementation. This, the second GAO report, has (1) determined the status of DOD's efforts to develop and implement a risk management approach to ensure the availability of DIB assets, and (2) identified challenges DOD faces in its approach to risk management. GAO

analyzed plans, guidance, and other documents on identifying, prioritizing, and assessing critical domestic and foreign DIB assets and held discussions with DOD and contractor officials.

0042 **Niska, Richard W., and Catharine W. Burt, *Emergency Response Planning in Hospitals, United States: 2003-2004,* Centers for Disease Control and Prevention, August 20, 2007. 13pp.**

This study presents baseline data to determine which hospital characteristics are associated with preparedness for terrorism and natural disaster in the areas of emergency response planning and availability of equipment and specialized care units. Information from the Bioterrorism and Mass Casualty Preparedness Supplements to the 2003 and 2004 National Hospital Ambulatory Medical Care Surveys was used to provide national estimates of variations in hospital emergency response plans and resources by residency and medical school affiliation, hospital size, ownership, metropolitan statistical area status, and Joint Commission accreditation.

0055 **Executive Office of the President, *National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-related Information Sharing,* Executive Office of the President, October 2007. 42pp.**

Improving information sharing in the post-September 11 world requires an environment that supports the sharing of information across all levels of government, disciplines, and security domains. While this Strategy describes the vision that has guided the Administration for the past six years, it also sets forth our plan to build upon progress and establish a more integrated information sharing capability to ensure that those who need information to protect our Nation from terrorism will receive it and those who have that information will share it. We will improve interagency information sharing at the Federal level, while building information sharing bridges between the Federal Government and our non-Federal partners. The National Strategy for Information Sharing takes its lead from the President's National Security Strategy, which provides the broad vision and goals for confronting the national security challenges of the 21st century. In addition, it is closely aligned with the National Strategy for Combating Terrorism and the National Strategy for Homeland Security. This Strategy also supports and supplements the National Implementation Plan, which is the foundational document guiding the efforts of the Directorate of Strategic Operational Planning in the National Counterterrorism Center. Finally, this Strategy aligns with the National Intelligence Strategy, published at Presidential direction by the Director of National Intelligence in October 2005. An information sharing framework is recognized as a critical component of intelligence reform in the National Intelligence Strategy.

0097 **Young, Charles P., *Method or Madness: Federal Oversight Structures for Critical Infrastructure Protection,* Naval Postgraduate School, December 2007. 75pp.**

Telecommunications is one of the most critical national infrastructures, enabling many other infrastructure sectors to function. The federal oversight for this sector, put in place by the Department of Homeland Security, relies heavily on voluntary cooperation between the public and private sectors. Given that no large-scale disruption of the nationwide telecommunications backbone has occurred, there is no empirical evidence showing the effectiveness of the structure DHS has put in place. In an effort to gauge the effectiveness of

the various existing infrastructure oversight structures, this thesis examines four specific roles assumed by the federal government and their performance in their respective sectors. These roles and sectors are Owner (aviation), Customer (power), Coordinator (local telecommunications), and Regulator (food). Each case is reviewed to determine the effects of the government role on economic impact of the disruption, the time required to restore initial operating capabilities, and the time required to restore full operating capabilities. The various cases show that the government role has little direct impact on the costs related to infrastructure disruptions. The Regulator role had a negative impact on timeliness for both initial and full restoration. The other roles all made positive contributions to both restoration timeliness.

0171 **Elias, Bart, *National Aviation Security Policy, Strategy, and Mode-specific Plans: Background and Consolidations for Congress*, Congressional Research Service, Library of Congress, January 2, 2008. 28pp.**

The 9/11 Commission concluded that the terrorist attacks of September 11, 2001, revealed failures of imagination, policy, capabilities, and management by both the Federal Aviation Administration (FAA) and the U.S. intelligence community. Following the September 11, 2001, attacks, U.S. aviation security policy and strategy was closely linked to the changes called for in the Aviation and Transportation Security Act (ATSA, P.L. 107- 71), which emphasized sweeping changes to the security of passenger airline operations. While the importance of strategic planning was recognized, it was not a priority. The 9/11 Commission Report concluded that the TSA had failed to develop an integrated strategy for the transportation sector and mode specific plans, prompting Congress to mandate the development of these strategies and plans in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108- 458). While the TSA has developed these strategies and plans, the documents have been considered security sensitive thus limiting public discourse on the DHS strategy for aviation security. However, in June 2006 President Bush directed the DHS to establish and implement a national strategy for aviation security and an accompanying set of supporting plans.

0199 **Gallagher, Jerry P., *Reducing the Threat of Terrorism Through Knowledge Sharing in a Virtual Environment between Law Enforcement and the Private Security Industry*, Naval Postgraduate School, March 2008. 97pp.**

Each day approximately 6,800 members of the private security workforce are deployed across Kansas City to provide protection services at venues, many of which have been identified as being critical infrastructure and/or key resources. While these guards are tasked with providing the first line of defense at these locations, there is currently no mechanism or protocol in place to facilitate a timely exchange of threat information between private security and the KCPD. To empower this resource as a terrorism prevention force multiplier the development of a web based virtual knowledge sharing initiative was explored in this study as a solution to provide "one stop shopping" for consumers of homeland security related needs from the private security industry. The factors measured in this study indicate that private security leaders perceived significant value in the proposed initiative and that the current environment is one that would favor success. One factor that supports this finding was the strong positive bias displayed to the "trust" factor, which was identified in this research as the lubricant of exchange relationships. While leaders did not demonstrate a high level of concern regarding the threat of a local terrorist act occurring in the next five years,

the sharing of threat information did indicate that complacency could be reduced and the level of interest/value of participating be increased through the sharing of threat knowledge. Industry leaders also clearly indicated a universal belief that private security should have a role in the mission of countering critical infrastructure.

0295 **Wilson, Clay, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*, Congressional Research Service, Library of Congress, March 26, 2008. 20pp.**

Electromagnetic Pulse (EMP) is an instantaneous, intense energy field that can disrupt at a distance numerous electrical systems and high technology microcircuits that are especially sensitive to power surges. A large-scale EMP effect can be produced by a single nuclear explosion detonated high in the atmosphere. This method is referred to as High-Altitude EMP (HEMP). A similar, smaller scale EMP effect can be created using non-nuclear devices with powerful batteries or reactive chemicals. This method is called High Power Microwave (HPM). Several nations, including sponsors of terrorism, may currently have a capability to use EMP as a weapon for cyberterrorism to disrupt communications and other parts of the U.S. critical infrastructure. Some equipment and weapons used by the U.S. military may be vulnerable to the effects of EMP. The threat of an EMP attack against the United States is hard to assess, but some observers indicate that it is growing along with worldwide access to newer technologies and the proliferation of nuclear weapons. In the past, the threat of mutually assured destruction provided a deterrent against the exchange of multiple high-yield nuclear warheads. But now even a single, specially designed low-yield nuclear explosion high above the United States, or over a battlefield, can produce a large-scale EMP effect that could result in a widespread loss of electronics, but no direct deaths, and may not necessarily evoke a large nuclear retaliatory strike by the U.S. military. This, coupled with the possible vulnerability of U.S. commercial electronics and U.S. military battlefield equipment to the effects of EMP, may create a new incentive for other countries to develop or acquire a nuclear capability.

0315 **Federal Emergency Management Agency, *Incremental Protection for Existing Commercial Buildings from Terrorist Attack: Providing Protection to People and Buildings*, Federal Emergency Management Agency, April 2008. 166pp.**

The Federal Emergency Management Agency (FEMA) developed FEMA 459, Incremental Protection for Existing Commercial Buildings from Terrorist Attack, to provide guidance to owners of existing commercial buildings and their architects and engineers on security and operational enhancements to address vulnerabilities to explosive blasts and chemical, biological, and radiological hazards. It also addresses how to integrate these enhancements into the ongoing building maintenance and capital improvement programs. These enhancements are intended to mitigate or eliminate long-term risk to people and property.

0481 **General Accountability Office, *Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets*, U.S. Government Accountability Office, April 2, 2008. 18pp.**

As part of GAO's ongoing work, this report evaluates the extent to which DOD is (1) identifying and prioritizing critical Sensitive Compartmented Information (SCI) and Special Access Programs (SAP) assets in Defense Critical Infrastructure Program (DCIP) and (2)

assessing critical SCI and SAP assets for vulnerabilities in a comprehensive manner consistent with that used by DCIP for collateral-level assets. GAO conducted this performance audit from September 2007 through February 2008 in accordance with generally accepted government auditing standards.

0499 **Bas, Ali, and Volkan Karaca, *A Simulation on Organizational Communication Patterns during a Terrorist Attack*, Naval Postgraduate School, June 2008. 79pp.**

The purpose of this project is to provide a simulation which includes communication structures during a terrorist attack. Different communication patterns will provide different results in terms of effectiveness and efficiency. We are planning to identify some key variables to form an effective network structure in a military action. According to key variables of an organization, centralized and decentralized structures produce different communication patterns and different outputs as well. In a combat environment these different patterns will result in distinct results in terms of effectiveness and efficiency. This environment can be modeled by the help of software like Arena. As a part of the Global War on Terrorism NATO forces are conducting operations in Afghanistan. To enhance stability in Afghanistan, NATO established PRTs (Provincial Reconstruction Teams) composed of multinational elements (partly civilian, but mostly military. These teams are static, and form potential targets for terrorist attacks. We will use PRTs in our model as the target of the terrorists and try to discriminate communication structures in these ambush scenarios.

0577 **Government Accountability Office, *Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks*, U.S. Government Accountability Office, June 2008. 26pp.**

Technological advances have led to an increasing convergence of previously separate networks used to transmit voice and data communications. While the benefits of this convergence are enormous, such interconnectivity also poses significant challenges to our nation's ability to respond to major disruptions. Two operations centers—managed by the Department of Homeland Security's (DHS) National Communications System and National Cyber Security Division—plan for and monitor disruptions on voice and data networks. In September 2007, a DHS expert task force made three recommendations toward establishing an integrated operations center that the department agreed to adopt. To determine the status of efforts to establish an integrated center, GAO reviewed documentation, interviewed relevant DHS and private sector officials, and reviewed laws and policies to identify DHS's responsibilities in addressing convergence.

0603 **Scovell, Calvin L., III, *Actions Needed to Enhance Pipeline Security*, Department of Transportation, June 25, 2008. 11pp.**

The Nations pipeline infrastructure is a network of approximately 2 million miles of pipelines that move millions of gallons of hazardous liquids and billions of cubic feet of natural gas daily. Within the United States, there are about 2,200 natural gas pipeline operators and 300 hazardous liquids pipeline operators. DOTs Pipeline and Hazardous Materials Safety Administration (PHMSA) is responsible for overseeing the safety of the Nations pipeline system. The Transportation Security Administration (TSA) within DHS is responsible for securing the Nations transportation infrastructure, including pipelines.

Safeguarding the Nation's massive pipeline infrastructure from catastrophic events (i.e., terrorism or natural disasters) is a continuing challenge for DOT and DHS.

0614 **Copeland, Claudia, *Terrorism and Security Issues Facing the Water Infrastructure Sector,* Congressional Research Service, Library of Congress, July 28, 2008. 22pp.**

This report presents an overview of the nation's water supply and water quality infrastructure, describes security-related actions taken by the government and the private sector since September 11th, and discusses additional policy issues and responses, including congressional concerns.

0636 **Blatus, Richard J., *Altering the Mission Statement: The Training of Firefighters as Intelligence Gatherers,* Naval Postgraduate School, September 2008. 70pp.**

The fire service is one of the premier emergency response agencies in the United States. As our nation strives to expand and enhance its homeland security efforts, firefighters have been recognized as an underutilized asset. The opportunity for firefighters to act as "first preventers" in the war on terrorism is unmatched by any other emergency response agency. This, coupled with the warrantless search provisions afforded firefighters by the Constitution, makes firefighters the logical choice for training and inclusion into an expanded terrorism awareness initiative. Expansion of the intelligence-gathering capabilities of first responders, specifically firefighters, will not be without difficulty. The lack of training and educational opportunities afforded firefighters in this area, the changes in fire fighting culture, the status of firefighters as an integral part of the community, are all obstacles that must be addressed. Firefighters respond to homes and businesses with unprecedented frequency. A multi-faceted approach involving training, community involvement, and operational awareness will streamline the utilization of firefighters in the area of threat recognition. Trained firefighters will help shoulder some of the burden placed on law enforcement while the utilization of a current asset will put forth a new best practice for the safety of our communities.

Nuclear Terrorism

0706 **Richardson, J., et al., *Improved Technology to Prevent Nuclear Proliferation and Counter Nuclear Terrorism,* Lawrence Livermore National Laboratory, June 15, 2006. 10pp.**

As the world moves into the 21st century, the possibility of greater reliance on nuclear energy will impose additional technical requirements to prevent proliferation. In addition to proliferation resistant reactors, a careful examination of the various possible fuel cycles from cradle to grave will provide additional technical and nonproliferation challenges in the areas of conversion, enrichment, transportation, recycling and waste disposal. Radiation detection technology and information management have a prominent role in any future global regime for nonproliferation. As nuclear energy and hence nuclear materials become an increasingly global phenomenon, using local technologies and capabilities facilitate incorporation of enhanced monitoring and detection on the regional level. Radiation detection technologies are an important tool in the prevention of proliferation and countering radiological/nuclear terrorism. A variety of new developments have enabled enhanced performance in terms of energy resolution, spatial resolution, passive detection, predictive modeling and simulation, active interrogation, and ease of operation and deployment in the field. For example, various

gamma ray imaging approaches are being explored to combine spatial resolution with background suppression in order to enhance sensitivity many-fold at reasonable standoff distances and acquisition times. New materials and approaches are being developed in order to provide adequate energy resolution in field use without the necessity for liquid nitrogen. Different detection algorithms enable fissile materials to be distinguished from other radioisotopes.

0716 **Dunlop, W. H., and H.P. Smith, *Who Did It? Using International Forensics to Detect and Deter Nuclear Terrorism*, Lawrence Livermore National Laboratory, September 13, 2006. 11pp.**

Although Washington has naturally focused on preventing a nuclear terrorism attack in the United States, a U.S. city is not necessarily the most likely target for nuclear terrorists. It is doubtful that a terrorist organization would be able to acquire a U.S. nuclear device and even more doubtful that it would acquire one on U.S. soil. Accordingly, if a terrorist organization does get its hands on a fission device, it is likely that it will do so on foreign territory. At that point, the terrorists will have an enormously valuable political weapon in their hands and will be loath to risk losing that asset. Given the risks associated with getting the device into the United States, the rational choice would be to deploy the device abroad against much softer targets. For Islamist terrorists, a major "Christian" capital such as London, Rome, or Moscow might offer a more suitable target.

0727 **Eack, Kevin D., *Securing Nuclear and Radiological Material in the Homeland*, Naval Postgraduate School, March 2007. 99pp.**

It is well established among the intelligence community that terrorists view the acquisition of nuclear or radiological materials (NRAM) as a goal in furtherance of their efforts to attack the U.S. within its borders. The use of NRAM in a nuclear weapon of mass destruction (WMD) or a radiological dispersion device (RDD) could potentially kill and injure thousands of American citizens. The economic impact of such a terrorist act on U.S. soil could cause profound economic damage, and would terrify the nation. While international efforts have been underway for many years to better secure military nuclear weapons and materials, this research finds that a comprehensive national security strategy in the U.S. for commercial nuclear materials is needed. While some strides were made in 2005 through measures taken by the U.S. Nuclear Regulatory Commission (NRC) to better secure nuclear generating power facilities, there is no similar comprehensive security strategy for NRAM stored or being transported in the U.S. This poses a potentially serious threat to our homeland security. This research reviews the present statutory and regulatory scheme for NRAM, and outlines a dramatic new approach that will better ensure our homeland security.

0826 **Arbuckle, Larry J., *The Deterrence of Nuclear Terrorism Through an Attribution Capability*, Naval Postgraduate School, June 2008. 64pp.**

The state of the world is such that the pace of nuclear weapons proliferation appears to be increasing. The growing number of nuclear states and amount of nuclear material available poses a great challenge to those who would attempt to keep nuclear weapons out of the hands of terrorists and other non-state actors. This study examines how the development of a nuclear attribution capability using the tools and methods of nuclear forensics can address that challenge. The prevention of nuclear terrorism is a multi-front battle. One of these fronts

is preventing state sponsorship of nuclear terrorism. This can best be accomplished through deterrence policies that threaten severe and credible military action against would-be nuclear sponsors. However, such threats only have meaning if the sponsors are convinced that their participation could be detected. Therefore, there is a need for a credible means to determine the source of nuclear materials from the debris of a nuclear explosion. At present a national nuclear forensics capability is lacking. There is a need for a more robust database of known nuclear materials, as well as for organizational restructuring and equipment development.

0890 **Department of Homeland Security, *Nuclear/Radiological Incident Annex*, U.S. Department of Homeland Security, June 2008. 32pp.**

The Nuclear/Radiological Incident Annex (NRIA) to the National Response Framework (NRF) describes the policies, situations, concepts of operations, and responsibilities of the Federal departments and agencies governing the immediate response and short-term recovery activities for incidents involving release of radioactive materials to address the consequences of the event. These incidents may occur on Federal-owned or -licensed facilities, privately owned property, urban centers, or other areas and may vary in severity from the small to the catastrophic. The incidents may result from inadvertent or deliberate acts. The NRIA applies to incidents where the nature and scope of the incident requires a Federal response to supplement the State, tribal, or local incident response.

0922 **Shea, Dana A., *The Global Nuclear Detection Architecture: Issues for Congress*, Congressional Research Service, Library of Congress, July 16, 2008. 25pp.**

The U.S. government has implemented a series of programs to protect the nation against terrorist nuclear attack. These programs have historically been viewed as lacking coordination and centralized oversight. In 2006, the Domestic Nuclear Detection Office (DNDO) was established within the Department of Homeland Security to centralize coordination of the federal response to an unconventional nuclear threat. The office was given specific statutory responsibilities to protect the United States against radiological and nuclear attack, including the responsibility to develop a global nuclear detection architecture. Determining the range of existing federal efforts protecting against nuclear attack, coordinating the outcomes of these efforts, identifying overlaps and gaps between them, and integrating the results into a single architecture are likely to be evolving, ongoing tasks. The global nuclear detection architecture is a multi-layered system of detection technologies, programs, and guidelines. Among its components are existing programs in other federal agencies and new programs put into place by DNDO. The global nuclear detection architecture is developed by DNDO in coordination with other federal agencies; this coordination is essential to the success of the architecture. The DNDO is developing risk and cost methodologies to be applied to the architecture in order to understand and prioritize the various nuclear detection programs and activities in multiple federal agencies. Congress, in its oversight capacity, has shown interest in the development and implementation of the global nuclear detection architecture. Other issues that may be foci of attention include the balance between investment in near- and long-term solutions, the degree and efficacy of federal agency coordination, the mechanism for setting investment priorities in the architecture, and the efforts DNDO has undertaken to retain institutional knowledge regarding this sustained architecture effort.

0947 **Finlay, Brian D.,** ***Nuclear Terrorism: U.S. Policies to Reduce the Threat of Nuclear Terror,*** **Partnership for a Secure America, September 2008. 28pp.**

The study below acknowledges that the US government has taken important steps to prevent nuclear proliferation and to detect and interdict the international transfer of potentially dangerous nuclear materials. Yet it also finds that US government money and authority remains overly stove-piped within agencies, and poor interagency coordination hampers overall policy effectiveness. At the other end of the policy process, foreign government partners often do not share US goals and expectations, while investments in sustainable and transparent civilian opportunities for WMD experts are inadequate, undermining long-term US goals.

0976 **Homeland Security Council,** ***Planning Guidance for Response to a Nuclear Detonation,*** **Homeland Security Council, January 16, 2009. 96pp.**

The purpose of this guidance is to provide emergency planners with nuclear detonation-specific response recommendations to maximize the preservation of life in the event of an urban nuclear detonation. This guidance addresses the unique effects and impacts of a nuclear detonation such as scale of destruction, shelter and evacuation strategies, unparalleled medical demands, management of nuclear casualties, and radiation dose management concepts. The guidance is aimed at response activities in an environment with a severely compromised infrastructure for the first few days when it is likely that many Federal resources will still be en route to the incident.

RELATED COLLECTIONS

Studies in Global Crises

- **Weapons of Mass Destruction and Nonproliferation**
- **International War on Drugs**

Radical and Reactionary Politics in America

- **Series 1: The American Radicalism Collection**
- **Series 2: Radicalism, Reaction and Dissent: Selections from the Hall Hoag Collection**

FBI File on Posse Comitatus