NAVAL WAR COLLEGE
Newport, R.I.

FINDING THE DEMONS IN OUR MIDST:

UTILIZING DOD ISR ASSETS TO COMBAT TERRORIST USE OF CBRNE WEAPONS

by

Sean R. Liedman

Lieutenant Commander, United States Navy

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

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

04 February 2002

_____

CDR Erik J. Dahl, USN
Professor of Joint Military Operations

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
04 Feb 2002	N/A	-

Title and Subtitle Finding the Demons in Our Midst: Utilizing DOD ISR Assets to Combat Terrorist Use of CBRNE Weapons	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes
The original document contains color images.

Abstract
The horrific terrorist attacks of September 11, 2001 on the U.S. homeland highlighted the threat that terrorism poses to U.S. national security. DoD operates globally a large network of Intelligence, Surveillance, and Reconnaissance (ISR) assets which could be brought to bear in the effort to combat terrorism. The geographic Commanders-in-Chief (CINCs) set the priorities for the intelligence networks in their Areas of Responsibility (AORs) according to their interpretation of the strategic guidance from the National Command Authority (NCA). A key tenet of the new strategic setting is the grave threat to national security posed by terrorism, potentially using Chemical, Biological, Radiological, Nuclear, or Enhanced High Explosive (CBRNE) weapons. This fact, coupled with the new strategic mandate that sets defense of the homeland as the highest priority for the U.S. military, dictates that each of the geographic CINCs set combatting terrorist use of CRBRNE weapons as the highest priority for their intelligence networks. The success or failure of this operational intelligence effort could have major strategic effects.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified

Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 24	

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: **JOINT MILITARY OPERATIONS DEPARTMENT**	
6. Office Symbol: C	**7. Address**: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): FINDING THE DEMONS IN OUR MIDST: UTILIZING DOD ISR ASSETS TO COMBAT TERRORIST USE OF CBRNE WEAPONS. (UNCLASSIFIED)	
9. Personal Authors: LCDR Sean R. Liedman, USN	
10.Type of Report: FINAL	**11. Date of Report**: 04 FEBRUARY 2002
12.Page Count: 24	**12A Paper Advisor (if any):** CDR Erik J. Dahl, USN, JMO Faculty
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: Intelligence, Surveillance, Reconnaissance, Terrorism, Chemical, Biological, Radiological, Nuclear, Homeland, Defense.	

15.Abstract: The horrific terrorist attacks of September 11, 2001 on the U.S. homeland highlighted the threat that terrorism poses to U.S. national security. DoD operates globally a large network of Intelligence, Surveillance, and Reconnaissance (ISR) assets which could be brought to bear in the effort to combat terrorism. The geographic Commander's-in-Chief (CINCs) set the priorities for the intelligence networks in their Areas of Responsibility (AORs) according to their interpretation of the strategic guidance from the National Command Authority (NCA). A key tenet of the new strategic setting is the grave threat to national security posed by terrorism, potentially using Chemical, Biological, Radiological, Nuclear, or Enhanced High Explosive (CBRNE) weapons. This fact, coupled with the new strategic mandate that sets defense of the homeland as the highest priority for the U.S. military, dictates that each of the geographic CINCs set combatting terrorist use of CRBRNE weapons as the highest priority for their intelligence networks. The success or failure of this operational intelligence effort could have major strategic effects.

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		**20.Office Symbol:** C	

ABSTRACT

FINDING THE DEMONS IN OUR MIDST: UTILIZING DOD ISR ASSETS TO COMBAT TERRORIST USE OF CBRNE WEAPONS

The horrific terrorist attacks of September 11, 2001 on the U.S. homeland highlighted the threat that terrorism poses to U.S. national security. DoD operates globally a large network of Intelligence, Surveillance, and Reconnaissance (ISR) assets which could be brought to bear in the effort to combat terrorism. The geographic Commander's-in-Chief (CINCs) set the priorities for the intelligence networks in their Areas of Responsibility (AORs) according to their interpretation of the strategic guidance from the National Command Authority (NCA). A key tenet of the new strategic setting is the grave threat to national security posed by terrorism, potentially using Chemical, Biological, Radiological, Nuclear, or Enhanced High Explosive (CBRNE) weapons. This fact, coupled with the new strategic mandate that sets defense of the homeland as the highest priority for the U.S. military, dictates that each of the geographic CINCs set combatting terrorist use of CBRNE weapons as the highest priority for their intelligence networks. The success or failure of this operational intelligence effort could have major strategic effects.

> On September 11th, 2001, the United States came under vicious, bloody attack. Americans died in their places of work. They died on American soil. They died not as combatants, but as innocent victims. They died not from traditional armies waging traditional campaigns, but from the brutal faceless weapons of terror. They died as the victims of war – a war that many had feared but whose sheer horror took America by surprise.
>
> - Secretary of Defense Donald H. Rumsfeld[1]

The U.S. has experienced six major international terrorist attacks since the World Trade Center bombing of 1993, culminating in the recent horrific attack by the Al Qaeda terrorist network on September 11th, 2001 in which more than 3,000 people from over 60 nations were killed.[a] The "911" attack achieved an unprecedented scale of death and destruction in the history of terrorism, yet the magnitude of this terrorist incident pales in comparison with the potential consequences and casualties in scenarios that involve terrorist employment of Chemical, Biological, Radiological, Nuclear, or Enhanced High Explosive (CBRNE) weapons. The Department of Defense (DoD) employs globally a large network of Intelligence, Surveillance, and Reconnaissance (ISR) assets which could be brought to bear in the effort to combat terrorist use of CBRNE weapons, and the current strategic setting dictates that this effort be elevated to the highest priority for the U.S. military. Historically, geographic Commanders-in-Chief (CINCs) have viewed terrorism through the lens of Antiterrorism/Force Protection (AT/FP), as they are charged to do in U.S. joint doctrine. However, the presence of international terrorist cells in North Africa presents more than an AT/FP problem for the military forces deployed in the European Command (EUCOM) and Central Command (CENTCOM) Areas of Responsibility (AOR's); they present a threat to the homeland and the geographic CINC's must combat them as part of a coordinated homeland defense effort. Each of the geographic CINCs should increase the priority of

---

[a] For the purposes of this paper, the six major international terrorist attacks are considered to be the World Trade Center Bombing of 1993, the Khobar Towers Bombing of 1995, the African Embassy bombings of 1998 (Tanzania and Kenya), the USS COLE bombing of 2000, and the September 11th terrorist attack on the United States in 2001. The State Department lists eighty-three "significant" terrorist incidents during this time period.

intelligence collection and analysis efforts to combat terrorism in their theater intelligence planning. The success or failure of this operational intelligence effort to combat terrorism in each of the CINC's AORs could have major strategic effects for the United States.

Clearly, a comprehensive strategy for combatting terrorism will require a unified effort that encompasses all of the instruments of national power including diplomatic, informational, economic, and military entities. Terrorism has been traditionally regarded as a crime, and thus DoD does not have lead agency responsibility for combatting terrorism. Presidential Decision Directive 39 (PDD 39), "U.S. Policy on Counterterrorism," dated 21 June, 1995 spelled out lead agency responsibility for terrorist incidents and remains the governing document for interagency coordination as of this writing. [2] Under PDD-39, the Department of Justice (DoJ) is the lead agency for domestic terrorism and the FBI is the lead agency within DoJ for operational responses to terrorist incidents. The Federal Aviation Administration (under the Department of Transportation) is the lead agency for terrorist incidents that occur aboard an aircraft in flight. The U.S. Coast Guard (under the Department of Transportation) is the lead agency for responding to terrorist actions that occur in maritime areas subject to U.S. jurisdiction. DoD is the lead agency for carrying out a program to provide civilian personnel of federal, state, or local agencies with training and expert advice regarding emergency responses to use or threatened use of a weapon of mass destruction or related materials.[3] President George W. Bush established the Office of Homeland Security by executive order on 8 October 2001, and charged it with the following mission:

> The mission of the Office shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. The Office shall perform the functions necessary to carry out this mission, including the functions specified in section 3 of this order.[4]

This new agency may change these interagency relationships in the effort to combat terrorism, but as of this writing it is not yet clear how that will occur. This paper will not

examine the merits of different organizational approaches to combatting terrorism, nor will it focus on the strategic intelligence efforts of the national intelligence community, executed by agencies such as the Central Intelligence Agency (CIA). Rather, it will focus on the operational intelligence capabilities that geographic CINC's can provide to the unified effort for combatting terrorism (particularly terrorist use of CBRNE), recognizing that DoD is not necessarily the sole or primary means to achieve U.S. policy objectives in combatting terrorism. This paper will utilize the definition of "combatting terrorism" contained in Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Anti-terrorism:"

> those actions (including antiterrorism and counterterrorism) taken to oppose terrorism throughout the entire threat spectrum. Antiterrorism involves **defensive measures** used to reduce the vulnerability to terrorist acts, as opposed to counterterrorism which consists of **offensive measures** taken to prevent, deter, and respond to terrorism. [Emphasis in original][5]

The New Strategic Setting

The "911" terrorist attack unquestionably altered the strategic setting for the United States. In order to understand the impact of the new strategic setting on the operational employment of military forces, the linkage between the strategic and operational levels must be examined. Joint Pub 3-0, "Doctrine for Joint Operations," states the following:

> National security strategy and national military strategy (NMS), shaped by and oriented on national security policies, provide strategic direction for combatant commanders. **Combatant commanders, in turn, provide guidance and direction through their combatant command strategies and plans for the employment of military forces, in conjunction with interagency and multinational forces, in the conduct of military operations**. [Emphasis added.][6]

Having established the primacy of the National Security Strategy (NSS) and NMS in determining strategic priorities for the combatant commanders (the CINC's), the strategic tenets of the NSS and NMS must be examined next. The last NSS was published by the Clinton administration in December 2000, and the last NMS was published in 1997. The most recent strategic guidance from the current presidential administration is contained in the

Quadrennial Defense Review Report of 2001 (QDR 2001). It lays out the following two strategic principles that are relevant to this topic:

1. Defense of the homeland is the #1 strategic priority for DoD. QDR 2001 explicitly and repeatedly states this as demonstrated by the following passages:

> The highest priority of the U.S. military is to defend the Nation from all enemies. The United States will maintain sufficient military forces to protect the U.S. domestic population, its territory, and its critical defense-related infrastructure against attacks emanating from outside U.S. borders, as appropriate under U.S. law. U.S. Forces will provide strategic deterrence and air and missile defense and uphold U.S. commitments under NORAD. In addition, DoD components have the responsibility, as specified in U.S. law, to support U.S. civil authorities as directed in managing the consequences of natural and man-made disasters and CBRNE-related events on U.S. territory. Finally, the U.S. military will be prepared to respond in a decisive manner to acts of international terrorism committed on U.S. territory or the territory of an ally.[7]

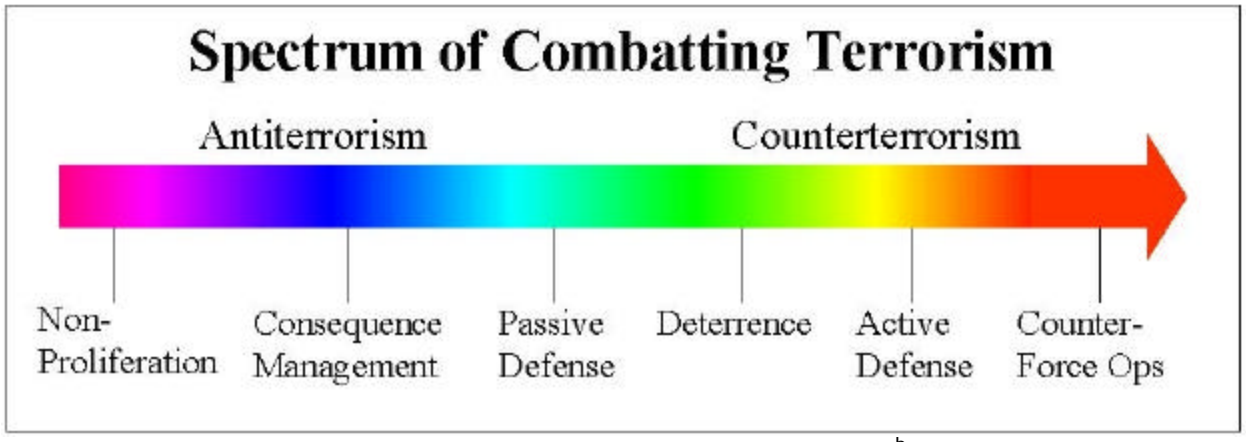
> Defending the nation from attack is the foundation of strategy. As the tragic September terror attacks demonstrate, potential adversaries will seek to threaten the centers of gravity of the United States, its allies, and its friends… Therefore, the defense strategy restores the emphasis once placed on defending its land, sea, air, and space approaches.[8]

2. Terrorism is a serious threat to the homeland. QDR 2001 also clearly outlines the gravity of the strategic threat to the homeland that terrorism poses:

> The attacks against the U.S. homeland in September, 2001 demonstrate that terrorist groups possess both the motivations and capabilities to conduct devastating attacks on U.S. territory, citizens, and infrastructure. Often these groups have the support of state sponsors or enjoy the sanctuary and protection of states, but some have the resources and capabilities to operate without state sponsorship. In addition, the rapid proliferation of CBRNE technology gives rise to the danger that future terrorist attacks might involve such weapons.[9]

QDR 2001 clearly sets defense of the homeland as the number one priority for U.S. military forces and recognizes that terrorism, potentially using CBRNE weapons, constitutes a serious threat to the homeland. This leads to the next question: How can DoD forces be employed to defend the homeland against terrorist CBRNE threats? The strategies for

protecting the homeland from terrorist CBRNE attack fall along a spectrum ranging from non-proliferation through counter-force operations as shown below in Figure 1:



- Figure 1[b]

While none of these strategies are mutually exclusive of the others, they each need to be examined independently as they will result in different courses of action for DoD forces.

Non-proliferation. Non-proliferation is an integral tool for reducing the likelihood of terrorist use of CBRNE weapons, and DoD forces support non-proliferation efforts as stated in Joint Pub 3-11, Joint Doctrine For Operations In Nuclear, Chemical and Biological (NBC) Environments:

> In shaping a peaceful international environment favorable to US interests, US policies and strategies seek to prevent and limit the proliferation of NBC capabilities through international agreements and treaties, multilateral initiatives, and unilateral actions. The Armed Forces of the United States support these policies and strategies within their respective roles and functions.[10]

There are a number of international treaties in place that seek to prevent proliferation, including the Treaty on The Non-proliferation of Nuclear Weapons, the Chemical Weapons Convention (CWC), and the Biological Weapons Convention. There are three basic problems that have limited the effectiveness of non-proliferation schemes. The first is that not all nations are signatories to these treaties; for example, 20 nations, including Iraq, Libya,

[b] This spectrum was conceived and illustrated by the author based on research from multiple sources.

and North Korea, have not signed the CWC.[11] Second, there is a general lack of credible inspection processes to ensure compliance. The final problem is that the treaties govern nation-states; non-state actors such as terrorist organizations are not signatories and therefore may not consider this form of international law binding. Thus, while non-proliferation will continue to be a cornerstone of U.S. policy, it is insufficient in and of itself to protect the U.S. homeland from CBRNE attack.

Consequence Management. Consequence management (CM) attempts to limit the effects of a CBRNE incident, both through pre-planned responses and crisis management. Joint Task Force-Civil Support (JTF-CS) was created in October of 1999 under Joint Forces Command (JFCOM) and given responsibility for CM. JTF-CS's mission statement is:

> JTF-CS at Joint Forces Command will plan and integrate Department of Defense (DoD)'s support to the Federal Emergency Management Agency (FEMA) for Weapons of Mass Destruction (WMD) events in the Continental United States (CONUS). This support will involve capabilities drawn from throughout the Department, including detection, decontamination, medical, and logistical assets. Regarding deployment, when ordered, JTF-CS deploys to the vicinity of a WMD incident site in support of the Lead Federal Agency, establishes command and control of designated (DoD) forces and provides military assistance to civil authorities to save lives, prevent human suffering, and provide temporary critical life support.[12]

Consequence management is a critical element of combatting CBRNE terrorism, but it is a reactive concept that **does not defend** the U.S. from CBRNE attack. It must be combined with other strategies to effectively defend the homeland.

Passive Defense. Current DoD doctrine for passive NBC defense centers on the three principles of contamination avoidance, protection, and decontamination.[13] Contamination avoidance requires detecting the presence of CBRN hazards and minimizing personnel exposure. Protection of individuals is usually accomplished collectively through NBC shelters, or individually through protective garments and breathing apparatus. These methods may be a suitable passive defense solution for a fielded force of 500,000 military

personnel such as the U.S. deployment to the Arabian Gulf in 1991. However, passive defense is certainly not a practical solution for a country of 280 million people dispersed across more than 3.7 million square miles. It is simply too large of an area with too many people to train and equip for personal protection. Some of these principles such as contamination avoidance could be applied by employing NBC detection devices near major urban areas. This would aid in determining the extent of contamination of a CBRN attack, and help to minimize the number of people that are exposed. Again, though, this is a limited effort that would only minimize - not prevent - the effects of a CBRN attack.

Deterrence. PDD-39 states:

> The United States shall seek to deter terrorism through a clear public position that our policies will not be affected by terrorist acts and that we will act vigorously to deal with terrorists and their sponsors. Our actions will reduce the capabilities and support available to terrorists.[14]

"Joint Doctrine Capstone and Keystone Primer" states:

> Demonstrated military capability is the cornerstone of deterrence, which remains a principal means for dissuading would-be aggressors and adversaries from action harmful to the United States."[15]

However, the jury is still out on the efficacy of punishment deterrent strategies vis-a-vis terrorism. Paul Pillar, in his book Terrorism and U.S. Foreign Policy, lists three reasons why military retaliation may not serve as an effective deterrent to future terrorist operations:

> First, the terrorists most likely to threaten U.S. interests present few suitable military targets, especially high-value targets whose destruction would be very costly to the terrorists… Second, nonphysical effects of a military strike may serve some of the political and organizational purposes of terrorist leaders, and for that reason they may tacitly welcome such an attack… Third, the terrorists' response to a retaliatory strike may be counter-retaliation rather than good behavior.[16]

The U.S. retaliatory cruise missile strikes in 1998 following the African embassy bombings failed to deter Al Qaeda from executing the USS COLE (DDG-67) and "911" attacks. The magnitude of the U.S.-led military coalition response in Afghanistan following the "911"

attacks may change the deterrent calculus for other terrorist organizations and the states harboring them, but that is undetermined as of this writing.

These four counterterrorism strategies, singularly or in combination, will not adequately ensure that the homeland will be defended from terrorist CBRNE attack. Thus, a concerted effort to defend the homeland must include two more aggressive strategies – active defense and counterforce operations.

Active Defense and Counterforce. Joint Pub 3-11 clearly states the necessity of active defense and possibly counterforce operations to supplement passive NBC defense:

> While a necessary part of the solution to the NBC threat, passive NBC defense is insufficient in and of itself. In addition to passive defense measures, neutralizing the threat will require effective application of other military capabilities, in particular active defense measures and counterforce operations.[17]

Some military examples of active defense include Ballistic Missile Defense (BMD) and Defensive Counter Air (DCA), both of which can reduce the number of incoming missiles or aircraft, thereby reducing the number of CBRNE weapons that threaten friendly personnel and territory. However, military forces are not the only solution for active CBRNE defense. Civil agencies such as the FBI and the U.S. Customs Service can play an important role in defending the U.S. against terrorist CBRNE attack through covert or unconventional means of delivery such as commercial cargo shipments, passenger aircraft, or private vehicles and vessels. The apprehension of Ahmed Ressam by a U.S. Customs agent in December of 1999 in Port Angeles, Washington foiled a terrorist attack on Los Angeles International Airport and serves as a perfect example of a civil law enforcement agency conducting active defense against terrorism.[18]

The same can be said of counterforce operations; the U.S. military has many offensive weapons in its arsenal that are capable of striking directly at the heart of terrorist organizations. Strike aircraft, cruise missiles, and direct action by Special Forces are some

examples. However, there are other counterforce options available besides U.S. military force, including covert action and military or law enforcement action by the host nation.

The actual disruption, apprehension, or destruction of the terrorists and their threatening schemes in active defense or counterforce strategies (the "end game") may be undertaken by civil or military agencies and is beyond the scope of this paper. What is relevant to this paper is the fact that effective active defense and counterforce operations versus CBRNE terrorism depend on **intelligence**, as stated in Joint Pub 3-07.2:

> Intelligence and counterintelligence are the first line of defense in an AT program. A well-planned, systematic, all-source intelligence and counterintelligence program is essential. The role of intelligence is to identify the threat, provide advanced warning, and disseminate critical intelligence in a usable form for the commander. Additionally, counterintelligence provides warning of potential terrorist attacks and provides information for CT operations.[19]

A Credible CBRNE Threat?

Is there a credible terrorist CBRNE threat to the United States homeland? If so, by whom? What means of CBRNE will they use? Where? When?

To establish the existence of a credible CBRNE threat, it must be demonstrated that terrorists possess both the will and the means to carry out a CBRNE terrorist incident. The facts are clear that there exist some terrorist organizations that do have the will to carry out an attack on the United States, using CBRNE if possible. The "911" attack caused mass destruction, even though the terrorists did not employ the traditional CBRN weapons that are normally categorized as WMD. That attack was carried out by the Al-Qaeda terrorist organization, and masterminded by Usama bin Laden. In his "Declaration of the World Islamic Front for Jihad against the Jews and Crusaders" published in the Arabic newspaper Al-Quds al-Arabi on 22 February 1998, bin Laden stated:

> To kill Americans and their allies, both civil and military, is an individual duty of every Muslim who is able, in any country where this is possible…[20]

This statement coupled with the string of terrorist attacks committed by his Al-Qaeda network against the U.S. and its allies clearly demonstrates their resolve to commit these acts. However, do they seek to employ CBRNE? Bin Laden has made statements that demonstrate affirmative intent:

> Acquiring weapons for the defense of Muslims is a religious duty. If I have indeed acquired these weapons, then I thank God for enabling me to do so. And if I seek to acquire these weapons, I am carrying out a duty. It would be a sin for Muslims not to try to possess the weapons that would prevent the infidels from inflicting harm on Muslims.[21]

The Washington Post reported that Pakistani intelligence discovered that two retired Pakistani nuclear scientists met with bin Laden in the Afghan capital of Kabul and discussed nuclear, biological, and chemical weapons with him. The two scientists stated that bin Laden indicated that he had obtained, or had access to, some type of radiological material that he said had been acquired for him by the radical Islamic Movement of Uzbekistan.[22] Bin Laden and Al-Qaeda are but one clear example of the CBRNE terrorist threat.

The "What?" part of this question is partially answered by the acronym CBRNE – Chemical, Biological, Radiological, Nuclear, and Enhanced high explosive weapons. While there are significant technical hurdles (the Canadian Security Intelligence Service publication "Chemical, Biological, Radiological, and Nuclear Terrorism" provides a good discussion of these challenges) that terrorists must overcome to effectively employ CBRNE weapons the question seems to be not "if" but "when" these challenges will be solved.[23] A brief description of each of the CBRNE weapons follows, along with historical examples of terrorist employment of these weapons.

Chemical. Chemical weapons are generally defined as the use of a toxic poison such that the chemical effects on exposed personnel result in incapacitation or death.[24] The Aum Shinrikyo terrorist group chemical attack in the Tokyo subway system in March of 1995 released an estimated 159 ounces of Sarin between 5 subway trains, resulting in twelve

deaths and over 5,500 casualties reporting to medical treatment facilities.[25] It took four hours and fifteen minutes for Japanese health officials to conclusively determine that Sarin was the causative agent.[26] However, the Aum Shinrikyo attacks demonstrated the difficulty of dispersing a sufficiently lethal quantity over a large area to produce "mass" casualties. Aum Shinrikyo's relatively rudimentary dispersal method was aided by the fact that it was conducted in the enclosed environment of a subway. Effective dispersal over an open-air area (such as a large urban center) would be much more problematic.

Biological. A biological weapon is generally defined as the use of a pathogen to induce incapacitation or death.[27] However, the most daunting challenge for a terrorist to employ biological weapons is the same as the chemical weapons challenge: dispersal. Contagious agents do not suffer from this problem, but non-contagious agents such as anthrax must be widely dispersed in order to cause mass casualties. Aum Shinrikyo failed in ten known attempts in Japan to conduct biological attacks with either anthrax or botulinum toxin. Despite the cult's vast resources (approximately $1 billion) and access to trained scientists, it has been unable to overcome the technical hurdles associated with the acquisition, cultivation, and delivery of biological weapons.[28]

Radiological. Radiological weapons, also known as "dirty bombs" or Radiological Dispersal Devices (RDD's), are notionally conceived as conventional high explosive devices that disperse radioactive material in order to create a radiation hazard to humans. In 1995, Chechen rebels placed a 30-pound container of radioactive cesium in a Moscow park.[29] The device was intended to produce psychological shock rather than physical harm, and Russian officials quickly removed and disposed of the device without any serious harm. However, the incident underscored the potential dangers of a radiological terrorist attack and demonstrated that U.S. non-proliferation policies have not been 100% effective. Since 1993, the International Atomic Energy Agency has tracked 175 cases of trafficking in nuclear

materials and 201 cases of trafficking in radioactive materials used for medical and industrial purposes. Only eighteen of these cases involved plutonium or highly enriched uranium, the "weapons-usable" material that is required to make a nuclear bomb – the material in all other cases would have been suitable only for radiological weapons.[30]

Nuclear. Nuclear weapons present significant technological challenges for terrorists, which helps to explain why the world has not yet witnessed a terrorist nuclear attack. Rose Gottemoeller, then Assistant Secretary for Nonproliferation and National Security in the Department of Energy, provided the following assessment of the terrorist nuclear threat in testimony before the Senate Subcommittee on International Security, Proliferation and Federal Services and the Committee on Governmental Affairs:

> A simple nuclear device of the Hiroshima design is actually not the easiest nuclear capability for a proliferator to acquire, be he a terrorist or a rogue state actor. Although the design is now almost fifty years old, the Hiroshima device, also called a "gun-type" weapon, requires a large amount of nuclear material to achieve a nuclear explosion. We assume that 15-30 kg of highly enriched uranium or 3-4 kg of plutonium are needed for a sophisticated nuclear weapon. Cruder devices may require more. One estimate, for example, places the likely size of a Pakistani weapon at around 1,500 pounds. Therefore, although achieving a workable trigger device and other components would not be a trivial matter, the principal barrier to acquiring a nuclear weapon is the large amount of weapons-usable material that is needed.[31]

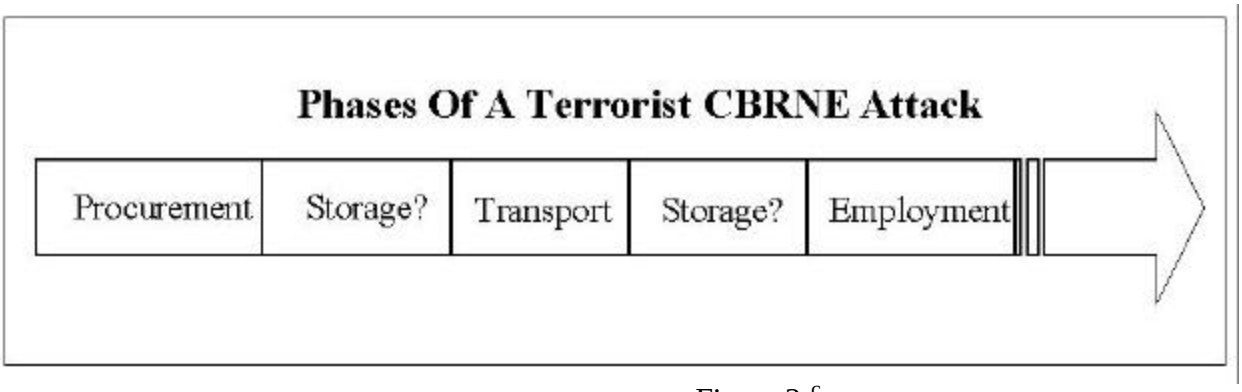
However, it is not beyond the realm of the possible for a terrorist organization to acquire and employ a nuclear device.

Enhanced High Explosive With Mass Consequences. The term "Enhanced High Explosive" has many different conceptualizations. Fuel-Air Effect (FAE) weapons are examples of enhanced high explosives, but in a terrorism context the term generally means any weapon that produces enhanced effects beyond those of a normal conventional explosive device. In this sense, flying an airliner in the World Trade Center could be defined as an enhanced high explosive, as it would have

required an extremely large conventional explosive to achieve the level of destruction that the "911" attack achieved.

Where and When?

The questions of "Where?" and "When?" are precisely the questions that the ISR network can potentially answer, regardless of the endgame chosen to counter the threat. Part of the where and when question is answered by examining the phases of manufacture, storage, and transportation prior to employment of a terrorist CBRNE attack as depicted in Figure 2:



- Figure 2.[c]

CBRNE weapons tend to be complex to manufacture, store, and employ, and therefore terrorist organizations usually require technical support from one of two sources – states that have the technology to manufacture CBRNE weapons, or private "enablers" - individuals who have experience in developing CBRNE weapons. These are important factors for the intelligence effort to combat terrorism, as they increase the "footprint" of the terrorists' operations and increase surveillance and reconnaissance opportunities for ISR assets.

The $64,000 question is, who provides the ISR on terrorist CBRNE threats? We've already examined the fact that DoJ has lead agency responsibility for domestic terrorism. DoJ has an extensive domestic intelligence network resident in the FBI and associated state and local law enforcement agencies. The problem with this relationship in combatting terrorism is that potentially the first three phases of a terrorist CBRNE attack may occur outside of the U.S.,

where DoJ has very little surveillance capability. DoS has lead agency authority for international terrorist incidents; however, DoS possesses even less surveillance capability than the FBI. If left to this arrangement alone to combat terrorism, intelligence gathering would commence at the U.S. borders and be supplemented only with whatever information foreign nations would be willing to divulge. Clearly, this arrangement is insufficient to provide the indications and warning required to mount an effective active defense and perform counterforce operations if necessary. However, the National Intelligence Community and DoD operate large, global, ISR networks on a daily basis and have the capability to provide global counter-terrorism ISR. The National Intelligence Community specifically has counterterrorism listed as one of its tasks in Executive Order 12333, United States Intelligence Activities:

> (c) Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotics activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;…[32]

However, at the operational level of intelligence, the geographic CINCs and their subordinate Joint Force Commanders (JFCs) do not have any written imperative to counter terrorism in their Area Of Responsibility other than from an AT/FP perspective. Rather, they are free to set the ISR priorities in their theater through Priority Intelligence Requirement's (PIRs), that are in theory determined by the CINC's translation of the NMS for his AOR.

Two counterarguments to this thesis emerge at this point. The first is that the CINC's ISR networks are already tasked to the maximum and cannot absorb yet another demand on their ISR assets. Low Density/High Demand (LD/HD) ISR platforms such as RC-135's, EP-3E's, U-2's, and JSTAR's are already over-utilized and cannot support increased tasking in support of counterterrorism. The second counterargument is that these traditional ISR platforms

---

[c] This diagram was conceived and illustrated by the author based on research from multiple sources

bring little detection capability to counter chemical and biological weapons development because of the difficulty in detecting these agents. The answer to the first counterargument is contained in the strategic imperative outlined above. The ISR community is over-tasked – but the strategic imperative of defending the homeland against terrorism demands that ISR support for that effort be elevated to the highest priority. Each of the geographic CINCs must then determine which of the other intelligence priorities will be downgraded in scope and effort. The answer to the second counterargument lies in the fact that while it may be difficult to detect the actual CBRNE agent, these traditional ISR platforms have an excellent capability to collect intelligence on the "footprint" required to manufacture, store, transport, and employ CBRNE weapons.

JFCOM's Unique Challenges. The thesis of this paper asserted that **all** geographic CINCs have been given a strategic imperative by QDR 2001 to gather operational intelligence on terrorism in their AOR's as a means of defending the homeland. U.S. Joint Forces Command (JFCOM) has two unique legal barriers to accomplishing this mission: Posse Comitatus and intelligence oversight.

The Posse Comitatus Act of 1878 prohibits use of Army and Air Force personnel to execute the civil laws of the U.S. except in cases and under circumstances expressly authorized by the Constitution or an Act of Congress.[33]

The principle of intelligence oversight is spelled out in Executive Order 12333 to protect US citizens and their private property from intelligence gathering activities of the U.S. military and CIA. The FBI and the Justice Department have exclusive responsibility for domestic surveillance, under the jurisdiction of the courts.

> Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in

> accordance with procedures established by the head of the agency concerned and approved by the Attorney General. [34]

The "911" attacks demonstrated that there exists a credible terrorist threat to the homeland which threatens national security. It may be time to rethink Posse Comitatus and Intelligence Oversight. The U.S. has not experienced a major hostile foreign military presence on its soil since the War of 1812; the relevance of these two statutory provisions would not be called into question if the armed forces of a foreign power once again set foot on U.S. soil. Is there a distinction between a terrorist threat to the homeland and the armed forces of a foreign power? This question needs to be examined further.

Recommendations for the Geographic CINC's

The following recommendations are concluded from this paper.

1. Geographic CINCs should ensure that combatting terrorism, particularly using CBRNE weapons, receives the highest priority in the PIRs for their AOR. This will drive intelligence collection, analysis, and dissemination efforts to enhance the effectiveness of combatting terrorism across the entire spectrum of strategies, ranging from non-proliferation to counterforce operations. This elevation in priority will help to defend the homeland against terrorist attack and provide the added benefit of improving AT/FP in their AORs.

2. The CINCs should demand the procurement of advanced CBRN detection technology to aid in the effort to detect the manufacture, storage, transport, and employment of CBRN weapons. While this might be considered primarily a Title X responsibility for each of the services in the Planning, Programming, and Budgeting System (PPBS) process, the CINCs can influence the PPBS process by increasing the priority of CBRN detection equipment on their Integrated Priority Lists (IPLs). This would improve the effort to combat terrorist use of CBRN and also improve NBC capability in a traditional state-on-state conflict in their AOR.

3. The CINCs should improve interagency and combined counterterrorism intelligence coordination. This must occur not only in the CINC's interface with the various national intelligence agencies, but also between the CINCs and other federal agencies such as the FBI, within the bounds established by law. Additionally, the CINCs often have unique relationships with key combined and allied intelligence services – they should increase counterterrorism intelligence cooperation to the maximum extent permissible. President Bush has mandated interagency cooperation in his Executive Order establishing the Office Of Homeland Security. The Office shall:

> …coordinate and prioritize the requirements for foreign intelligence relating to terrorism within the United States of executive departments and agencies responsible for homeland security and provide these requirements and priorities to the Director of Central Intelligence and other agencies responsible collection of foreign intelligence;…[35]

> …coordinate efforts to ensure that all executive departments and agencies that have intelligence collection responsibilities have sufficient technological capabilities and resources to collect intelligence and data relating to terrorist activities or possible terrorist acts within the United States, working with the Assistant to the President for National Security Affairs, as appropriate;…[36]

How the Office of Homeland Security will implement these changes is not yet clear.

What is clear is that the geographic CINCs have a strategic mandate to defend the homeland, and CBRNE terrorism is a serious threat to the homeland. The first step in combatting terrorism is to gain knowledge of the enemy - intelligence. The CINCs should elevate the collection of intelligence to combat terrorism to the top priority for their ISR networks. These demons must be found and dealt with harshly before they are able to wreak more destruction on the U.S and her allies.

ENDNOTES

[1] Donald H. Rumsfeld, "Foreword", Department of Defense, Quadrennial Defense Review Report (Washington, DC: 30 September 2001), III.

[2] President, Presidential Decision Directive 39, "U.S. Policy on Counterterrorism" (21 June 1995). <http://www.fas.org/irp/offdocs/pdd39.htm> [21 January 2002].

[3] Ibid.; Mike O. Lacey and Brian J. Bill, eds. Operational Law Handbook (Charlottesville, VA: 2001), Chapter 18, 4.

[4] President, Executive Order, "Establishing the Office of Homeland Security and the Homeland Security Council," Federal Register, 66, no. 196 (10 October 2001), 51812-51817. <http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html> [20 January 2002].

[5] Joint Chiefs of Staff, Joint Tactics, Techniques, and Procedures for Antiterrorism, Joint Pub 3-07.2 (Washington, DC: 17 March 1998), vii.

[6] Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Pub 3-0 (Washington, DC: 10 September 2001), viii.

[7] Department of Defense, Quadrennial Defense Review Report (Washington, DC: 30 September 2001), 18.

[8] Ibid., 14.

[9] Ibid., 5.

[10] Joint Chiefs of Staff, Joint Doctrine For Operations In Nuclear, Biological, and Chemical (NBC) Environments, Joint Pub 3-11 (Washington, DC: 11 July 2000), I-7.

[11] SIPRI Chemical and Biological Warfare Project web site. <http://projects.sipri.se/cbw/docs/cw-cwc-nonsig.html> [22 January 2002].

[12] Joint Task Force-Civil Support Home Page, U.S. Joint Forces Command Web Site. <http://www.jfcom.mil/jtfcs/index.html> [23 January 2002].

[13] Joint Chiefs of Staff, JP 3-11, III-11.

[14] President, PDD-39.

[15] Joint Chiefs of Staff, Joint Doctrine Capstone and Keystone Primer (Washington, DC: 10 September 2001), 2.

[16] Paul R. Pillar, Terrorism and U.S. Foreign Policy (Washington, DC: The Brookings Institution 2001), 104 – 105.

[17] Joint Chiefs of Staff, JP 3-11, III-13.

[18] "Ahmed Ressam's Millenium Plot", PBS web page. <http://www.pbs.org/wgbh/pages/frontline/shows/trail/inside/cron.html> [22 January 2002].

[19] Joint Chiefs of Staff, JP 3-07.2, V-1.

[20] Bernard Lewis, "License To Kill: Usama Bin Ladin's Declaration of Jihad," Foreign Affairs (November-December 1998), p. 15; quoted in Ahmed S. Hashim, "The World According to Usama Bin Laden," Naval War College Review, Vol. LIV, Number 4, (Newport, RI: Naval War College Press, Autumn 2001), 27.

[21] Osama Bin Laden, Interview, Time, 23 December 1998; quoted in Ahmed S. Hashim, "The World According to Usama Bin Laden," Naval War College Review, Vol. LIV, Number 4, (Newport, RI: Naval War College Press, Autumn 2001), 26.

[22] Kamran Khan and Molly Moore, "2 Nuclear Experts Briefed Bin Laden, Pakistanis Say", Washington Post, 12 December, 2001, sec. 1, 1.

[23] Canadian Security Intelligence Service, Chemical, Biological, Radiological and Nuclear Terrorism Report: #2000/02 (18 December 1999). <http://www.fas.org/irp/threat/200002e.htm> [22 January 2002].

[24] James Fitzsimonds, "Weapons of Mass Destruction: Considerations for the Operational Commander," (Unpublished Joint Military Operations Faculty Paper, U.S. Naval War College, Newport, RI), 6.

[25] Amy E. Smithson and Leslie Ann Levy, Ataxia: The Chemical and Biological Terrorism Threat and the US Response (Washington, DC: The Henry L. Stimson Center October 2000), 89 - 100. <http://www.stimson.org/cbw/pdf/ataxiaexecsum.pdf> [24 January 2002].

[26] Ibid., 93.

[27] Fitzsimonds, 10.

[28] Aaron Weiss, "When Terrorism Strikes, Who Should Respond?" Parameters, (Autumn 2001), 117-33. <http://carlisle-www.army.mil/usawc/Parameters/01autumn/Weiss.htm> [23 January 2002].

[29] James L. Ford, "Radiological Dispersal Devices: Assessing the Transnational Threat," Strategic Forum, National Defense University Institute for National Strategic Studies, Number 136, (March 1998). <http://www.csis-scrs.gc.ca/eng/miscdocs/200002_e.html> [22 January 2002]

[30] Rose Gottemoeller, "Statement," U.S. Congress, Senate, Committee on Governmental Affairs and the Subcommittee on International Security, Proliferation and Federal Services, Current and Future Weapons of Mass Destruction (WMD) Proliferation Threats: Hearings before the Committee on Governmental Affairs and the Subcommittee on International Security, Proliferation and Federal Services, 107th Congress, 1st sess., 7 November 2001. <http://www.senate.gov/~gov_affairs/110701gottemoeller.htm> [23 January 2002].

[31] Ibid.

[32] President, Executive Order, "United States Intelligence Activities," Federal Register, 46. (8 December 1981), 59941. <http://www.nara.gov/fedreg/codific/eos/e12333.html> [23 January 2002].

[33] Lacey and Bill, Operational Law Handbook, 10.

[34] President, Executive Order, "United States Intelligence Activities."

[35] President, Executive Order, "Establishing the Office of Homeland Security and the Homeland Security Council."

[36] Ibid.

BIBLIOGRAPHY

Canadian Security Intelligence Service. Chemical, Biological, Radiological and Nuclear Terrorism Report: #2000/02. Ottawa, Ontario, Canada: 18 December 1999.

Fitzsimonds, James. "Weapons of Mass Destruction: Considerations for the Operational Commander." Unpublished Joint Military Operations Faculty Paper, U.S. Naval War College, Newport, RI.

Ford, James L. "Radiological Dispersal Devices: Assessing the Transnational Threat," Strategic Forum, National Defense University Institute for National Strategic Studies, Number 136, (March 1998).

Hashim, Ahmed S. "The World According to Usama Bin Laden." Naval War College Review, (Autumn 2001): 11-35.

Lacey, Mike O. and Bill, Brian J., eds. Operational Law Handbook. Charlottesville, VA: 2001.

Pillar, Paul R. Terrorism and U.S. Foreign Policy. Washington, DC: The Brookings Institution 2001.

Smithson, Amy E. and Levy, Leslie Ann. Ataxia: The Chemical and Biological Terrorism Threat and the US Response. Washington, DC: The Henry L. Stimson Center, October 2000.

U.S. Congress. Senate. Committee on Governmental Affairs and the Subcommittee on International Security, Proliferation and Federal Services. Current and Future Weapons of Mass Destruction (WMD) Proliferation Threats: Hearings before the Committee on Governmental Affairs and the Subcommittee on International Security, Proliferation and Federal Services. 107th Congress, 1st sess., 7 November 2001.

U.S. Department of Defense. DoD Antiterrorism/Force Protection (AT/FP) Program. DoD Directive 2000.12. Washington, DC: 13 April 1999.

_____. Joint Service Chemical and Biological Defense Program: FY00-02 Overview. Washington, DC.

_____. Proliferation: Threat and Response. Washington, DC: January 2001.

_____. Quadrennial Defense Review Report. Washington, DC: 30 September 2001.

U.S. General Accounting Office. Combating Terrorism: Selected Challenges and Related Recommendations. Washington, DC: September 2001.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington, DC: 10 September 2001.

_____. Joint Doctrine For Operations In Nuclear, Biological, and Chemical (NBC) Environments. Joint Pub 3-11. Washington, DC: 11 July 2000.

_____. Joint Tactics, Techniques, and Procedures for Antiterrorism. Joint Pub 3-07.2. Washington, DC: 17 March 1998.

_____. Joint Doctrine Capstone and Keystone Primer. Washington, DC: 10 September 2001.

U.S. President. Executive Order. "Establishing the Office of Homeland Security and the Homeland Security Council." Federal Register 66, no. 196 (10 October 2001): 51812-51817.

_____. Executive Order. "United States Intelligence Activities." Federal Register 46, (December 8, 1981): 59941.

Weiss, Aaron. "When Terrorism Strikes, Who Should Respond?" Parameters, (Autumn 2001): 117-33.