THE TERRORIST THREAT AND ITS IMPLICATIONS FOR SENSOR TECHNOLOGIES

Jennifer L. Brower
Prometheus Inc.
Newport, RI 02840, USA

Abstract Recent terrorist attacks demonstrated that even sophisticated terrorists capable of planning and executing multiple, coordinated attacks continue to rely on traditional weapons rather than risk the uncertainty of chemical, biological, radiological or nuclear (CBRN) weapons. While some terrorist organizations have the motivations and capabilities to conduct large attacks worldwide, we have not yet witnessed the use of so called weapons of mass destruction (WMD) foreshadowed by the 1995 Sarin attacks in Tokyo, the discovery of al Qaeda's crude biological weapons program in Afghanistan, and the anthrax attacks in the United States in the fall of 2001. Anti-Western extremists pose a global threat, but what do the use of traditional weapons and innovative tactics mean for the future of terrorism? This chapter describes our current understanding of the global terrorist threat including the use of CBRN weapons. A discussion of the implications for sensor research, particularly for chemical and biological agents and radioactive materials then follows.

Keywords:
terrorism, al Qaeda, chemical terrorism, biological terrorism, radiological terrorism, nuclear terrorism, state sponsored terrorism, threat, sensors

1. Introduction

The deadly terrorist bombings of July 7, 2005 in London again demonstrated that even sophisticated terrorists capable of planning and executing multiple, coordinated attacks continue to rely on traditional weapons rather than risk the technical and political uncertainty of chemical, biological, radiological or nuclear (CBRN) weapons. While terrorists have the motivations and capabilities to conduct large (and small) attacks worldwide, we have not yet witnessed the use of so called weapons of

mass destruction (WMD) foreshadowed by the 1995 Sarin attacks in Tokyo, the discovery of al Qaeda's crude biological weapons program in Afghanistan, and the anthrax attacks in the United States in the fall of 2001. The strike on commuter trains in Madrid, Spain; the bombing of a nightclub in Bali, Indonesia; and the attacks of September 11, 2001 in the United States demonstrate that anti-Western extremists pose a global threat, but what do the use of traditional weapons and innovative tactics mean for the future of terrorism? This chapter describes our current understanding of the global terrorist threat including the use of CBRN weapons.

The threat described in the first part of this chapter spurred increased investment in research and development technologies to prevent, detect, and respond to terrorist attacks. One specific area of research, sensors, particularly for chemical and biological agents and radioactive materials, in addition to radar and sonar, is the subject of this book. After describing the threat, this chapter goes on to discuss the use of sensors, fielded sensor capabilities, and existing gaps in sensor capabilities.

2. What is Terrorism?

2.1 Definition

There is no single definition of terrorism, and even when one can agree upon a definition, there may be disagreements about the classification of a particular incident. This chapter is written from a U.S. perspective (as the author is from the United States) and the author refers the reader to the definition of terrorism as defined by statute of the United States Government (Title 22 Chapter 28 Section 2656 f(d)):

> Terrorism is premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.

2.2 History of Modern Terrorism

Modern terrorism is generally cited as beginning in the late 1960s with the emergence of an independent Israel. In the nearly four decades since, four categories of terrorist organizations have emerged — ideological, ethno-nationalist, politico-religious, and single issue. In the 1960s through 1980s terrorism was generally practiced by members of an identifiable group with clear goals. For example, leftist terrorist organizations such as the Red Army Faction (Baader Meinhof Gang) wanted to form additional socialist states in Europe, and ethno-nationalist groups such as the Abu Nidal Organization and the Irish Republican Army (IRA) wanted separate homelands for 'their' people. These types of organiza-

tions generally chose tactics and targets to achieve their political, social, or economic goals and claimed responsibility for their radical actions. As a result of decisions such as Roe v. Wade in the United States, and the emergence of fears of climate change and globalization, single-issue terrorism emerged in the late 1970s. It is broadly defined as "extremist militancy on the part of groups or individuals protesting a perceived grievance or wrong usually attributed to government action or inaction" [52]. In the late 1990s and early 2000s, animal rights and environmental activists were the most active domestic terrorists inside the United States in terms of number of attacks, but their belief system forbids harm to all animals (including humans) [30]. Later, groups began to emerge with less logical nationalist or ideological motivations, embracing instead more vague religious or millenarian objectives. The groups themselves were also less well defined [27]. Religious and millenarian groups such as al Qaeda and their affiliates and Aum Shinrikyo have grown to be the most dangerous terrorists based on their motivation to bring an end to modern civilization and their interest in WMD. We now turn to current thinking on the evolution of terrorism.

3. General Trends in Terrorism

Recent terrorist activity indicates that while the U.S. and its allies have enemies in many places, al Qaeda and its affiliates pose the greatest threat to Western interests. Al Qaeda — the World Islamic Front for Jihad Against the Jews and the Crusaders — is determined to bring an end to Western civilization as we know it. Note however that while the on-going attacks throughout the world are appalling in terms of the loss of human life and economic damage, the doomsday scenarios that many anticipated, involving massive casualties through the use CBRN weapons, have not materialized [22] and [37]. Lower consequence events are more likely than higher consequence events, primarily because of technical and logistical hurdles in executing large-scale attacks and because of counterterrorism efforts focused on avoiding mass attacks, but the risk of higher consequence events remains given the desire of al Qaeda (and others) to acquire or develop CBRN weapons.

A terrorism expert, Brian Jenkins, once noted, "Terrorists want a lot of people watching not a lot of people dead" [31]. At the time, only 15-20% of all terrorist incidents involved fatalities; however as early as 1987, he recognized the potential for increasing lethality. This was only one of the more recent trends he foresaw. Until the 1980s, terrorists often had specific goals for changing the behavior of a specific political body. With the evolution of religious extremism, the desensitization of terrorists and

the public, growing resources and other factors, terrorism has changed in many aspects. Terrorism experts and policy makers have examined changes in organization, motivation and capability (For instance see [22], [29], [48], and [56]. These trends were examined in the Fourth Report of the Gilmore Commission and are discussed and expanded below.

3.1 Increasing Lethality

First, selected terrorist groups are motivated and capable of killing more people in single or coordinated attacks than ever before. While the United States has been the target of terrorism for at least 35 years, more than three times as many people were killed on September 11, 2001 than in the history of modern terrorism until that day [28]. Worldwide, 14 modern terrorist operations achieved a death toll great than 100 before September 11 [32]. Since September 11, there have been several attacks with more than 100 deaths. In 2004 alone there were at least six attacks that claimed more than 100 lives each [16]. The most deadly was the Beslan school hostage crisis in Russia when 344 people were killed. Others include a TNT explosion on a ferry outside Manila which killed 118 (Abu Sayyaf Group); Ansar al-Sunnah's near simultaneous suicide attacks on two Kurdish Government targets in Arbil, Iraq, which killed 117; the slaughter by arson of 239 civilians in Northern Uganda by the Lord's Resistance Army; the multi-pronged bombing and mortar attack on the holy Shiite city of Karbala, which killed 106 (attack attributed to al Qaeda or Zarqawi loyalists, but no one claimed responsibility); and the bombing of commuter trains in Madrid Spain, which killed 191 and injured more than 600 (Abu Hafs Al Masri Brigade on behalf of al Qaeda). Other high casualty attacks include the October 2002 attack on a Bali nightclub and the Chechen attack on the Palace of Culture Theater that same month in which 162 were killed when the Russian Special Forces attempted to free the hostages using an incapacitating gas [41].

While there have been multiple attacks that have killed over 100 individuals, and despite the desire to carry out high profile mass casualty attacks, the arrests of key members of terrorist organizations have degraded al Qaeda's capability to conduct large attacks inside the United States and elsewhere. Several high casualty attacks were thwarted by law enforcement and intelligence agencies. For instance, in late 2001 intelligence from Afghanistan was used to detain 13 Jemaah Islamiyah (JI) members suspected of plotting to target U.S. Navy ships and sailors in Singapore. According to Gunaratna (2003), JI presents the largest terrorist threat in Southeast Asia with nearly 400 al Qaeda trained

members. Indonesia's tolerance has allowed a training infrastructure to thrive.

In addition, al Qaeda and its affiliates have lost several operational leaders, safe havens and sources of financing [56]. Those detained or arrested include, Khalid Sheik Muhammad, al Qaeda's operations chief and mastermind of the September 11 attacks (March 2003); Abd al-Rahim al-Nashiri, a senior operational planner in the Persian Gulf and mastermind of the USS Cole attack (November 2002); Abu Zubaydah, responsible for al Qaeda's recruitment and training and involved in the East African bombings in 1998 (March 2002); Omar al-Farouq, al Qaeda's operations chief in Southeast Asia (June 2002); Riduan Isamuddin, also know as Hambali, mastermind of the Bali bombings (August 2003); and Ibn al-Shaykh al-Libi, head of al Qaeda's training camps (December 2001). To avoid further disruptions to their attacks, terrorist groups have been forced to change tactics and targets.

3.2 Innovations in Tactics and Targets

Generally modern terrorist organizations have not been particularly innovative, often relying on a group of attack types and imitating other terrorist organizations. Even al Qaeda, an innovative group as described below, was influenced by a precursor, the Iranian-sponsored Lebanese Hezbollah, and particularly their ability to coordinate multiple attacks [24]. Al Qaeda has used coordinated, multiple attacks several times including the 1998 East Africa bombings; the September 11 attacks; and the bombings of the Interior Ministry and Recruiting Center in Riyadh Saudi Arabia in December of 2004. Affiliated terrorist groups have also imitated this tactic using multiple near-simultaneous bombings to kill scores of people. In Pakistan, the Muslim United Army simultaneously bombed 21 gas stations on May 15, 2003 using improvised explosive devices [24] and most recently on July 7, 2005 four bombs detonated nearly simultaneously across London. Also recently, in June 2005, four car bombs detonated in the early evening near Baghdad, Iraq killing at least 23 [8].

Bombings, assassinations, armed assaults, kidnappings, hijackings, and barricade and hostage incidents were the tactics used in nearly 95% of all terrorist attacks until 1987 [31]. This statistic remains in effect today. The arrest of key planners, and other disruptions, has forced al Qaeda and its affiliates to change tactics and targets and focus on smaller-scale, softer targets such as hotels, religious and holy sites, and infrastructure [20]. This is not the first time security changes have impacted tactics. For instance, terrorists commonly took control of em-

bassies in the 1970s, but as states implemented security measures, the seizures declined [31]. More recently, because of lessons learned from the Oklahoma City bombing in 1995 and the East African bombings in 1998, the U.S. secured the land access to its embassies and other government targets: al Qaeda then turned to maritime targets and attacked the USS Cole. After the U.S. decreased the vulnerability of maritime targets, al Qaeda used airliners to strike on September 11 [24]. Since September 2001, as the U.S. and others strengthened airline security, al Qaeda turned its attacks to the rail infrastructure in London and Madrid.

Because the United States has fortified its defenses, terrorists have increasingly attacked Western targets abroad. In June 2005, hotels in Indonesia were put on alert after the U.S. embassy released a statement indicating that they were the targets of an imminent terrorist attack. [1] And while no attack materialized in Indonesia, several other soft targets including a hotel in Kenya, (November 2002) and synagogues in Turkey (2003 and Tunisia (2002) have been attacked by al Qaeda. In May 2002, Abu Zubaydah reinforced the threat to soft targets, particularly places where large number of Americans gather [51].

Terrorists are also adapting technology to improve their tactics and targeting. For example, al Qaeda is adapting dual technologies such as airplanes and commercially available chemicals, agricultural fertilizers, and liquid propane and nitrogen [24]. The Tamil Tigers of Eelam (LTTE) has also tried to acquire microlite airplanes and built its own airstrip purportedly to conduct suicide missions from the air [50].

In another innovation that resulted, in part, from Bin Laden's observation of the economic damage that followed the September 11 attacks, terrorist groups are increasingly attacking economic targets. Evidence of al Qaeda's evolving strategy can be found in the tapes released periodically by Bin Laden and his associates. In a tape released on October 6, 2002, four days prior to the Bali bombing, Bin Laden and his lieutenant Ayman al-Zawahiri warned "By God, the youths of God are preparing for you things that would fill your hearts with terror and target your economic lifeline until you stop your oppression and aggression" [6]. Energy, particularly oil, has been specifically targeted. According to IntelCenter, an al Qaeda document translated in 2004 called for "hitting wells and pipelines that will scare foreign companies from working there and stealing Muslim treasures." For example, in October 2002 terrorists targeted a Malaysian oil tanker and killed a Bulgarian sailor off the cost of Yemen. Abdel Rahim Al-Nashiri, a key member of al Qaeda, reportedly financed the attack as well as the attack on the USS Cole. Nashiri was arrested in 2002. Bin Laden is also aware of the costs to defend against

potential terrorist attacks. In a tape released in late 2004, Bin Laden said, "...We are continuing this policy of bleeding America to the point of bankruptcy." [2]

The focus on economic targets is not completely new. As early as 1978, a Palestinian group called the Arab Revolutionary Army injected Israeli fruit exports with mercury to damage the Israeli economy. Officials and consumers found contaminated fruit in Holland, West Germany, Belgium and England [41]. The globalization of the world economy and the just-in-time logistics used in many Western countries has increased the visibility of economic disruption and therefore the appeal of this type of attack to terrorist groups.

3.3 Leaderless Resistance and Loose Networks

The successful disruption of al Qaeda described above has forced the group to decentralize further into a "loose collection of regional networks that operate more autonomously" [56]. A terrorist plot interrupted by U.S. and Singapore Intelligence in December 2001 demonstrates how a network of extremists from throughout Southeast Asia were willing to work in conjunction with al Qaeda leadership to plan an attack on several U.S. targets including the U.S. Embassy, a Navy ship, and Navy personnel [62]. JI was identified as the operational leader; however, eight of thirteen men arrested in January 2002 for connections to the plot had trained in al Qaeda camps in Afghanistan and Malaysia. Surveillance footage of the Singaporean targets was found in the home of an al Qaeda leader in Afghanistan, indicating close coordination between operatives in Southeast Asia and Afghanistan [62]. Although recent attacks in London bore the hallmarks of an al Qaeda attack, the quality and quantity of the explosives initially point to local militants, suggesting that the attack may have been loosely coordinated.

Cooperation in Southeast Asia is the most developed, but Islamic extremists in Central Asia, North Africa and even Europe and North America have also formed loose networks. For instance, in September 2002 the Islamic Movement of Uzbekistan (IMU) was formed, bringing together separatists from Kyrgyzstan, Tajikistan, Chechnya, and the Xingjiang Province of China [19].

Although Bin Laden's abundant resources, expertise, and agenda is attracting several groups to form loose networks, some terrorist groups have shied away from identifying themselves with Bin Laden to avoid being the focus of the war on terror or to focus on local goals. For example, when U.S. forces in Afghanistan killed several of its members, and its assets were frozen in late 2001, the Harakat ul-Mujahadeen split off the

al Almi faction (HUM-A). HUM wanted to focus on the local agenda in Jammu and Kashmir, while HUM-A wanted to continue to pursue Bin Laden's global jihad against the West. The more extreme HUM-A has gone on to attack Western targets including killing 10 French businessmen in Karachi and bombing the U.S. Consulate in Karachi in 2002 [41] and [22].

3.4 Incorporation of Technology

Terrorists are exploiting advances in information technology, such as email, the internet, encryption, and video/audio production, to coordinate internal communication and to spread their message for recruiting and fund raising purposes [25]. Terrorists are also using the internet in finance operations and to encourage hacking to deface Western websites or perpetrate denial of service attacks [46]. In late 2004, Imam Samudra, the convicted mastermind of the Bali nightclub bombing, directed compatriots to Indonesian language websites that contain instructions on online credit card fraud and money laundering [55]. This change has evolved in part as a reaction to the disruption of traditional modes of communication, financing, and safe havens. These innovations present both dangers and opportunities. While al Qaeda and others may garner support through the use of technology, the employment of information technology can be exploited for intelligence gathering [61]. Al Qaeda is aware of its vulnerabilities, and there is some evidence that al Qaeda has deliberately created noise in the system to overwhelm intelligence agencies trying to decipher terrorist communications [35]. Al Qaeda operatives have also use advanced encryption technology to prevent the Intelligence Community from gaining access to their plans. Even in the mid 1990s, Wahid El Hage used encryption to send secure e-mails while plotting the East Africa embassy bombings. Former Director of the U.S. Federal Bureau of Investigation (FBI) Louis Freeh testified as early as 1998 that "One of the most difficult challenges facing law enforcement is how rapidly criminals and terrorists — both domestic and international — adopt advanced technologies to thwart the ability of law enforcement to investigate those who wish to do harm to our Nation and its citizens. That is why encryption has become the most important issue confronting law enforcement" [23].

Terrorist exploitation of technology is further enhanced when groups share their technological advances with other groups both formally and informally. As noted above, Samudra aimed his exhortation to use the internet for fraud and money laundering at all jihadists working towards the downfall of the West.

3.5 Groups Working Together

Terrorist groups both with related and unrelated objectives are cooperating to various degrees, driven in part by the war on terrorism. In the past, organizations such as the Palestine Liberation Organization (PLO), the Provisional Irish Republican Army (PIRA), and the Basque Fatherland and Freedom (ETA) have worked together. The IRA also trained Revolutionary Armed Forces of Columbia (FARC) militants in Colombia, reportedly in exchange for $2,000,000, in the use of explosives [54].

Al Qaeda's direct training and its sharing of resources and expertise brings these interactions to the next level [22]. In response to the key arrests and the disruption of its own network, al Qaeda has reached out to foster its global impact. For instance, al Qaeda is cooperating with JI and the Moro Islamic Liberation Front (MILF) in Southeast Asia; Al Ithihad al Islami in the Horn of Africa; Al Ansar Mujahidin — Islamic International Brigade (Caucuses); the Tunisian Combatants Group in the Middle East; Jayah-e-Mohammad in South Asia; the Salafi Group for Call and Combat (GSPC) in North Africa, Europe and North America; and several other Islamist groups [24]. The interactions are beneficial to both sides. For example, al Qaeda supports a MILF-run training camp that both groups use to train themselves and others [12]. Even Sunni Muslim groups such as Hamas, al Qaeda, and Islamic Jihad are now cooperating with the Shiite Muslim group Hezbollah because of their shared hatred for the West, as evidenced by the issuance of joint press statements [22].

The interaction of multiple terrorist groups has also contributed to changes in tactics and targets. Al Ansar Mujahidin (Baryayev Gang) was clearly influenced by al Qaeda when it attacked the Moscow Theater in October of 2002. Movsar Baryayev, who was a close colleague of Ibn ul-Khattab, led the attack. Ibn ul-Khattab was a Chechen military leader, a protg of Bin Laden, and member of al Qaeda until his death in March 2002. Movsar utilized al Qaeda inspiration in the scale of the operation, the suicide potential, and the coordination [24]. The bombing of the nightclub in Bali grew from a local terrorist plot to conduct a number of small bombings on soft targets to the large-scale bombing after al Qaeda contributed bomb making expertise and resources to JI [24]. In general, al Qaeda's influence on Muslim ethno-nationalists is growing in the Philippines, Indonesia, Thailand, India-Pakistan and Russia through both imitation and the provision of direct training and resources. JI is a particularly good example of the impact al Qaeda has had. When the former Chief of JI in Singapore was arrested, he told investigators he

had been planning to hijack an Aeroflot plane from Bangkok and crash it into Singapore's main airport in 2002 to teach Russia a lesson — a clear emulation of the September 11 attacks. Further, the Bali attacks were both the first mass fatality and first suicide attack perpetrated by a Southeast Asian terrorist group — both as a result of contact with al Qaeda [24].

3.6 Threat of Individuals

Individuals acting without the support of a specific group, and who may sympathize with al Qaeda, the Palestinian cause, environmental causes or other grievances against the United States and its policies domestically or overseas also pose a threat. The threat from individual terrorists is increasing in part to the spread of propaganda and techniques and tools through the internet, and the threat is broader than that posed by al Qaeda and its affiliates [22]. For example Richard Reid, who was inspired by bin Laden, attempted to down an airliner over the United States using a shoe bomb [59]; the Egyptian, Hesham Mohamed Hadayet, killed two people at the El Al counter on July 4, 2002; and Osman Petmezci (Turkish) and Astrid Eyzaguirre (American) were stopped by German police before they could attack U.S. Army Headquarters in Heidelberg. After the arrests, police found 130 kg of bomb making components, related equipment, and a picture of Bin Laden in the couple's apartment [24]. Individual terrorists are harder to detect and stop, but they are also less likely to have sophisticated training or a wealth of resources and are therefore less likely to succeed. A particular threat in the United States is U.S. citizens who sympathize with international terrorist groups such as al Qaeda. Similar domestic threats pose challenges in other countries as well. It is to this threat that we now turn.

4. Significant Domestic Threats

While al Qaeda is considered the primary anti-Western terrorist organization, there are several other groups that have significant capabilities, and if their goals and motivations turned towards Westerners, defending against them would be a difficult endeavor. Locally these groups already present a challenge to the governments trying to protect their citizens. LTTE and FARC, two long-standing terrorist organizations, are discussed in this section because although they do not currently pose a global threat or have an anti-Western agenda, because of their organizational strength and capabilities they may pose a threat in the future.

The LTTE is one of the most deadly and persistent ethno nationalist/separatist organizations in the world. Born in 1976 out of the moderate Tamil United Liberation Front, their goal was to represent the Tamil minority in Sri Lanka and to create a separate state in the eastern and northern provinces. In addition to targeting the Sri Lankan government, LTTE has targeted civilians and other Tamil separatist groups. More than 60,000 people have been killed in the conflict since the mid 1970s with 514 fatalities attributed to the LTTE [41]. Driven in part by pressure from the global war on terrorism, the Sri Lankan government and the LTTE signed a cease-fire agreement on February 22, 2002. While the cease-fire generally held for all of 2003, violence resumed on July 8, 2004 when a female LTTE suicide bomber killed four policemen while attempting to assassinate Eelam People's Democratic Party member Douglas Devanda [41]. More recently, in February 2005, the LTTE leader Kausalyan was killed, reportedly by paramilitary Sri Lankan forces. This increase in violence has been driven by two factors: a split within LTTE over control of the Tamil vision between LTTE and another Tamil leader, Colonel Karuna and disagreement throughout Sri Lanka over the distribution of tsunami aid by the LTTE. The LTTE pose a significant local danger both in terms of the terrorist acts and in terms of recruiting children soldiers, but they have not turned their attention to the world of global terrorism or to WMD. In addition, the LTTE are well known for their innovations and adoption of technology, including the first use of women suicide bombers and their attempt to acquire microlite aircraft for terrorist attacks [49]. Continued vigilance is necessary because they are a sophisticated, organized group and splinter groups could become more radicalized. Or current interactions with Islamic terrorist groups such as Abu Sayyaf and the Moro Islamic Liberation Front could be exploited by any of the organization's splinter groups.

The FARC began as a Marxist organization determined to overthrow Columbia's government and replace it with a communist regime. The organization has wandered from its origins and increasingly focuses on the illicit drug trade and engaging in peace talks with the government. It now has more limited goals of controlling territory within the country. In addition to cocaine sales, the FARC uses kidnapping, extortion and hijacking to pad its coffers, reportedly taking in as much as $2 million per day. Its targets are private citizens and business with resources, rival communist terrorists, Columbian political and military entities, and rightist paramilitary forces. FARC does not present a direct threat to the United States, but its extensive drug trafficking network throughout the Americas, its significant resources, and its interactions with other

terrorists groups illustrate the potential for conducting significant attacks in the continental United States. This scenario will become more likely if increased cooperation among FARC and anti-Western extremists is observed, or if the U.S. war on drugs impacts their revenue stream.

4.1 Regional Assessment

The LTTE and the FARC represent two domestic threats. We now turn to an examination of some of the regions of the world with high levels of terrorist activity. According to the RAND/MIPT Terrorism Knowledge Database, the Middle East/Persian Gulf Region had both the largest number of incidents since the beginning of the new millennium and the highest number of injuries (13,663) and deaths (5,906). Almost 41% of the attacks and 75% of the deaths occurred in Iraq. Tanzim Qa'Idat Al-Jihad Fi Bilad Al-Rafidayn, a nationalist separatist group, has been one of the most prolific perpetrators since it was first mentioned in October of 2004. Israel, with 361 attacks and 681 deaths, and the Occupied Territories, with 1,607 attacks and 437 deaths, were also hit hard by terrorism. Hamas, Islamic Jihad, and Palestinian Islamic Jihad (PIJ) have perpetrated the vast majority of attacks both in Israel and in the Occupied Territories. East and Central Asia had the fewest attacks during this time period with 63 attacks and 63 deaths. Hamas presents some of the most violent opposition to Israel and has conducted numerous attacks using suicide bombers and rockets. It has caused nearly 600 deaths and 3000 injuries and is supported by Iran as well as numerous Islamic charities. PIJ is also dedicated to the destruction of Israel, but its actions have been reduced since the death of it leader Fathi Shaqai in 1995 and the start of the global war on terrorism [41].

Iraq's most infamous terrorist group is Tanzim Qa'idat al-Jihad Fi Bilad al Rafidayn (al Qaeda in Iraq), led by Abu Musab Zarqawi. This group has claimed responsibility for more than 100 attacks and 580 deaths with the stated goal of overthrowing the interim Iraqi Government, ridding the country of the American-led coalition, and forming an Islamic state. Recently, in May of 2005, multiple suicide bombers detonated blasts outside a courthouse in Baqubah killing several policemen and bystanders while attempting to kill the provincial governor of Diyala province. Tanzim Qa'idat al-Jihad Fi Bilad al Rafidayn is the successor to another deadly terrorist group, Tawhid and Jihad. This group is responsible for at least 25 incidents and nearly 200 fatalities. They used kidnappings, beheadings, assassinations and suicide bombings to move towards their goal of an Islamic State. Ansar al-Sunnah has been allied

with both of these groups, but commits deadly acts in its own name. For example, on May 11, 2005 the group perpetrated two fatal attacks - a car bombing in a Tikrit market near a police station that killed 38 and injured 84, and a suicide bombing that killed 32 recruits in Hawija. Ansar Al Islam, with similar goals, also operates within Iraq. Coalition forces decimated the organization's sanctuary in the Kurdish region of northern Iraq, and the group's leader, Mullar Krekar, was arrested in 2004 in Norway. However, Islamic jihadists are reportedly joining forces with the group, and in January of 2005, Ansar Al Islam perpetrated its first deadly attack in two years gunning down several Shiia religious leaders [41]. The number of terrorist groups allying themselves in Iraq demonstrates that Iraq is proving to be a fertile training ground and site for cross-fertilization.

Kashmir and Jammu, the disputed area between India and Pakistan is another active center of terrorist activity. Lashkar-E-Taiba (LeT), the militant arm of Markaz Dawa ul Irshad, along with Harkat ul Ansar (HuA) and Al-Badr (now known as Hizb ul Mujahidin) are responsible for much of the violence over the past 20 years. LeT is trying to establish Islamic rule over India and questions India's control of Jammu and Kashmir. As a member of Osama bin Laden's Islamic Front for Jihad against the U.S. and Israel, LeT poses a direct threat to U.S. interests, particularly in Pakistan and Afghanistan. Pakistan banned the group under pressure from the U.S., but it continues to operate. LeT relies on traditional terrorist arms and was blamed for the August 2003 bombing in downtown Bombay that killed 52 and injured more than 100 [41]. Hizb ul Mujahidin, the largest Kashmiri terrorist organization, is the militant wing of Pakistan's largest Islamic political group Jamaat-I-Islami. It primarily attacks political and military targets in Kashmir.

The Russian-Chechen conflict is another hotbed of terrorist activity. The Chechen terrorists, including the Movsar Naryayev Gang (MNG), support an independent Islamic Chechnya and are heavily influenced by radical Islam. The MNG was responsible for the well-publicized hostage taking at Moscow Theater in October 2002. When Barayev died in the attack, remnants of the group reportedly formed the extremely violent Riyad us-Saliheyn Martyrs' Brigade, which has claimed responsibility for the most heinous terrorist attacks in recent Russian history including the destruction of the pro-Russian Chechen government building in 2002 which killed 72, and an attack nearly a year later on a Russian hospital which killed 52. The group, like the LTTE, has also used women suicide bombers, both to bring down an airplane in August 2004 and to bomb Russian subways [41]. The group has strong ties to al Qaeda and is

willing to perpetrate large-scale attacks, and therefore poses a threat to the West.

As shown by the activity and aims of the terrorist groups discussed in this section, regional conflicts can directly affect Western security and safety, particularly as these conflicts fuel innovation and the interaction and training of multiple terrorist groups.

5. State Sponsored Terrorism

In addition to the organized and loose networks that generally fund their own activities, there are a number of states that sponsor terrorism. This is of particular concern with regards to weapons of mass destruction, because the numerous resources that can be brought to bear in state development of CBRN weapons can in turn be transferred to terrorists. Disincentives do exist to prevent this proliferation. As of October 2004, the United States lists six countries as state sponsors of terrorism: Cuba, Iran, Libya, North Korea, Sudan, and Syria. Of these, five are pursuing WMD to one degree or another. Libya repudiated its WMD program as discussed below.

Iran is a particular focus of the United States because of the convergence of its covert nuclear weapons program and its robust support of terrorism, going so far as to provide safe haven for the West's most threatening enemy, al Qaeda. In 2003, Iran refused to identify al Qaeda members in Iran or to transfer them to their countries of origin or third countries for detention and interrogation. Iran also provides material support including money, weapons, training and refuge to Hizballah, Hamas, PLFP, and Palestinian Islamic Jihad, and allowed terrorists fighting the coalition in Iraq, including members of Ansar al-Islam, to find safe haven within its borders. One of the members of its Guardian Council, the body that determines whether laws passed by the Iranian Parliament are in line with its constitution, promoted the idea of suicide attacks on coalition forces [47].

Iran is believed to have stockpiled chemical weapons and the means to deliver them. It is also believed to have a nascent biological weapons program, although it is unlikely to have sophisticated weaponized agents at this time. There is no question that Iran has acquired dual use biotechnology equipment, but the use of that equipment in the development of biological weapons has not been confirmed. Finally Iran's clandestine nuclear program is of greatest concern globally. Iran has violated its obligations under the non-proliferation treaty and International Atomic Energy Agency commitments several times. Violations include uranium enrichment; the creation of weapons grade plutonium; the development

of uranium mines and conversion facilities; and the construction of a heavy water production plant and several other hallmarks of a nuclear weapons program. These investments, purportedly for nuclear energy, are particularly unusual for an oil-rich state [11]. Iran's weapons are primarily directed at enemies such as Israel, but because of the country's status as the most active state sponsor of terrorism through 2003 [47] and its past and present association with terrorists, the threat must be closely monitored. The on-going debate about the background of Iran's newly elected President adds to the concern.

On the other hand, the threat from Libya has been significantly reduced since Moammar Gadhafi renounced his countries WMD aspirations in December of 2003. However, Libya remains on the list of state sponsors of terrorism. Prior to Libya's commitment to repudiate terrorism, it had supported some of the most deadly terrorist attacks including the bombing of Pan Am Flight 103 over Lockerbie, Scotland on December 21, 1988. But since Gadhafi's renunciation, documented progress has been made. By January 2004, U.S. and U.K. officials had removed critical elements of Libya's nuclear and long-range ballistic missile programs and consolidated its existing chemical weapons to protect them from terrorists and ease destruction [18].

Sudan was al Qaeda's primary operation base in the early and mid 1990s, and operatives from Sudan participated in the 1998 bombings of the U.S. embassies in Kenya and Tanzania, but the country is now working to combat terrorism and protect U.S. citizens within its borders. In 2003, the country shut down a major thoroughfare in front of the U.S. embassy in Khartoum to reduce the threat and closed a training camp, expelling several Saudi citizens training at the base [47]. Because Sudan possesses only a limited chemical capability and because of its recent cooperation with the U.S., it is unlikely that Sudan will deploy WMD through its limited terrorist network.

While North Korea poses a clear strategic threat to the United States and its allies, Kim Jong Il is not known to have directed any terrorist acts since the downing of Korean Air Flight 858 in 1987 in which 115 people were killed. Kim Jong was apparently trying to derail South Korea's Olympic events. However, because North Korea has nuclear, chemical and biological weapons capabilities and has supplied ballistic missile technology to other state sponsors of terrorism, it is unclear whether North Korea might provide materiel or technology for CBRN weapons to terrorist groups [57]. North Korea's primary motivation for selling ballistic missile technology to countries such as Iran and Syria appears to be the need for hard currency as opposed to specific anti-Western aims.

Syria has not directly participated in any known terrorist acts since 1986; however, Syria provides support and refuge for Hamas, the PIL, and the PFLP, among other Palestinian liberation groups. Syria distinguishes between what it calls the legitimate fight of the Palestinians and other terrorist groups. Syria also allows Iran to supply Hizbollah in Lebanon through its border, and with Iran reportedly supported Hizbollah's deadly bombing of the Marine Barracks and U.S. Embassy in Beirut in 1983. (Target America, 2001) The secular regime in Syria has begun to cooperate with the United States in its war against the Sunni dominated al Qaeda. Although Syria has a highly developed chemical weapons program and a less developed biological weapons program, and despite its sponsorship of anti-Western terrorism in the 1970s and 1980s, it is unlikely that Syria will share its chemical and biological capabilities with terrorist groups at this time. Syrian support now focuses on terrorism with limited political aims, and it prohibits anti-Western terrorism, limiting the threat to all but its primary target, Israel [47] and [58].

Cuba, while listed as a state sponsor of terrorism by the U.S. Government, does not provide significant resources or support for the most dangerous anti-western terrorists. Cuba is listed because it provides safe harbor to members of designated terrorist groups such as the Basque Fatherland and Liberty (ETA) and the FARC as well as other fugitives from U.S. justice [47].

Taken together, the on-going threat posed by state sponsors of terrorism has been reduced since the 1970s and 1980s when ideological and ethno-nationalist separatist groups aligned their fortunes with states; however, the future threat is significant, particularly if Iran or North Korea share their technological advances with groups they support, either because they share common goals or simply for financial gain.

6. Future Threats

Because so many national security experts and policy makers have predicted the use of CBRN weapons, it continues to be surprising that terrorists have been unable to follow through on their desires on a mass scale [22]. Technical and operational challenges present significant barriers to large-scale terrorist acquisition and use of CBRN l weapons [26]. Even al Qaeda, with its significant resources and global reach has not yet demonstrated the use of a sophisticated chemical or biological weapons capability. Based on videotapes discovered in Afghanistan and statements from Ahmed Ressam, the jailed terrorist who was planning to bomb the Los Angeles airport in December 1999, as of that time, al Qaeda was only capable of poisoning a trapped dog [22].

Arrests, the loss of sanctuary and the freezing of assets have diminished some threats, but it has spawned others as terrorists adjust to being the focus of the global war on terrorism. What will be the balance? Will loss of sanctuary and financial resources prevent terrorists from developing or acquiring CBRN that can be used to mass effect? Or will the global war on terrorism embolden terrorists and states to share and use CBRN? While terrorists continue to use traditional weapons in innovative ways, a primary concern is terrorist adoption of CBRN weapons in the future. The potential for this is explored next.

As discussed above, several states that support terrorism have some CBRN capabilities, so the technical constraint alone is not limiting. Rather, the potential backlash against any state that provides a terrorist organization with CBRN has been a sufficient deterrent to this point. However groups such as al Qaeda, Aum Shinrikyo, and the Tamil Tigers have shown significant interest in one or more types of unconventional weapons.

There can be no doubt that, if given the opportunity, terrorist groups such as al Qaeda would not hesitate to use disease as a weapon against the unprotected; to spread chemical agents to inflict pain and death on the innocent; or to send suicide-bound adherents armed with radiological explosives on missions of murder [10].

With the spread of information and the desperation for hard currency of some of the state sponsors of terrorism, as well as the changing national security environment, it is possible that terrorists may build or acquire CBRN in the future.

Bolton's opinion was bolstered in June 2005 by Senator Richard Lugar's survey of 85 non-proliferation and national security analysts from the United States and other nations. It was designed in part to characterize the risks related to the terrorist use of CBRN. The survey revealed that experts believe the probability of an attack somewhere in the world with a CBRN weapon was 50% over the next five years and 70% over the next ten. An attack with a radiological weapon was seen as the most probable with the likelihood of an attack with a nuclear or biological weapon considered about half as plausible [37]. The average probability of a nuclear attack in the next ten years was nearly 30%, with experts almost evenly divided between terrorist acquisitions of a working nuclear weapon versus self-construction [37]. The average risk estimate over ten years for major chemical and biological attacks was 20%. Senator Lugar concluded "The bottom line is this: for the foreseeable future, the United States and other nations will face an existential threat from the intersection of terrorism and weapons of mass destruction."

George Tenet, the former Director of Central Intelligence went even further in his February 2004 testimony before the Select Committee on Intelligence. "I have consistently warned this committee of al-Qaeda's interest in chemical, biological, radiological, and nuclear weapons. Acquiring these remains a 'religious obligation' in Bin Ladin's eyes, and al Qaeda and more than two dozen other terrorist groups are pursuing CBRN materials."

A number of trends discussed above favor the eventual use of CBRN weapons. The willingness to commit mass murder is primary among them. Cross fertilization among terrorist groups increases the likelihood that terrorists will develop and use more sophisticated tactics and weapons as groups share information and resources on materials, methods, and tactics. Splinter groups are seen as more likely to attempt innovation; and the spread of technology will put the power to develop ever more sophisticated weapons in the hands of terrorists.

To establish themselves as significant players in the political realm, splinter groups tend to be both more violent and more experimental than their parent groups. For example, Ansar al-Islam, a splinter from the Islamic Movement of Kurdistan (IMK) that associates with al Qaeda, established a lab in northern Iraq to manufacture and test chemical and biological agents, including ricin, for use in terrorist attacks [40].

There are several specific factors that indicate terrorist groups are making progress in the pursuit of CBRN materials and technology. A few highlights include:

- The wide dissemination of information across the internet by terrorists including instructions for improvised chemical weapons [56] and the open source information in scientific journals,
- The dissemination of anthrax in the United States in the fall of 2001,
- The discovery in January 2003 of remnants of ricin, castor beans, and recipes for a half dozen other chemical and biological weapons in the London apartments of terrorists aligned with al Qaeda,
- Unearthed terrorist documents in Afghanistan indicating al Qaeda's interest in nuclear, radiological, and biological weapons [56],
- Continuing discoveries of chemical precursors in Aum hideaways in Japan.

Al Qaeda in particular continues to pursue unconventional weapons, both leveraging existing commercially available agents and technologies and creating CBRN weapons. According to Rohan Gunaratna, "The

group is also searching for new weapons such as chemical and biological agents, especially contact poisons easy to conceal and breach security" [24]. However, contact poisons and the like are unlikely to cause the mass casualties often cited by U.S. security experts. Gunaratna also notes that a fatwa issued by Sheikh Nasr bin Hamid al Fahd in May 2003 legitimizes the use of CBRN weapons. Such a fatwa is a requirement in Islam before an attack. We can learn something about past and current terrorist capabilities and motivations by examining documented cases of actual use of chemical and biological weapons.

6.1 Actual Use of CBRN

Despite significant interest in unconventional weapons, there have been few instances of widespread death or incapacitation due to CBRN use by terrorists, and the number of casualties pales in comparison to those killed by more conventional explosives, armed attacks and arson. Since 1968, more than 14,000 people have been killed by bombing, and nearly 6,000 by armed attack, but CBRN attacks have accounted for less than 20 deaths [41]. The two most notorious unconventional attacks in modern history, Aum Shinrikyo's gassing of a Tokyo subway in 1995 and the anthrax attacks in the U.S. in the fall of 2001, killed a total of 17 people. The food poisoning by the Rajneeshees in Oregon in 1984 has also received much attention. While there were no fatalities when the cult poisoned several salad bars with Salmonella, there were more than 700 injuries.

The two known deadly attacks using either chemical or biological weapons are now discussed. In each of these incidents, less than 20 people were killed, but several hundred were injured in Japan. In both cases, the resulting fear and response led to much greater disruptions and costs than the attacks themselves.

Aum's story is an illustration of how a group with significant financial resources and educated personnel may still have a hard time surmounting the technological and organizational challenges to developing a true WMD. Aum Shinrikyo, which translates as the "Supreme Truth," is a Japanese religious cult led by Shoko Asahara. Asahara drew on Christianity, Buddhism, and Hinduism to create his own religion, which, at its peak, attracted up to 40,000 followers worldwide, primarily in Russia and Japan [41]. The group first attracted the significant attention of law enforcement in 1995 after it gassed the Tokyo subway, killing 12 and injuring hundreds. Its activities and interest in unconventional weapons began long before the attack. In the early 1990s, the cult had an estimated net worth in the hundreds of millions to a billion dollars and had a

cadre of scientists including 20 university-trained microbiologists. Aum provided these members with the necessary equipment and materials, and yet the group failed in ten attempts to kill large numbers of people with either anthrax or botulinum toxin. Their failure was attributed in part to the use of a non-lethal strain of anthrax and technical difficulties in disseminating the biological agents, which proved less hardy and stickier than anticipated. Aum also tried unsuccessfully to acquire nuclear weapons and materials from Russia as well as mine uranium in Australia. Aum then turned to developing chemical agents, and while the group successfully killed individuals in Matsumoto (in 1994 Aum targeted three judges with Sarin and killed seven) and Tokyo, they did not achieve the doomsday scenarios anticipated by Asahara and dreaded by U.S. and international leaders.

Even after the arrest of its leader and other key personnel, the Japanese government did not fully outlaw the sect and a small group of followers remain. The group also retains a large network of business and influence interests. In April 2004, the Japanese Justice Ministry's Public Security Investigation Agency released a report that indicated that Aum, renamed Aleph in 2000, had set up more than 10 businesses throughout Japan. The cult purports to raise money to help victims, but the Justice Ministry claims that these businesses are designed to raise money for Aum's operating expenses [34]. Armageddon remains the cults guiding concept and the Japanese government continued to discover Sarin precursor chemicals years after the 1995 attack [39]. With its sufficient resources, followers and motivations, Aum still poses a threat. They could prove even more threatening if they could enlist help from a State or if they could illicitly purchase needed technologies to support their goal of a successful mass attack. International intelligence and law enforcement must continue to carefully watch the cult that will not go away.

In the fall of 2001, letters containing a sophisticated and lethal form of powdered anthrax were sent to news media outlets and two democratic senators (the letters to the two senators were more highly refined and therefore more deadly). Of the eleven victims of inhalational anthrax, six survived. Eleven people also came down with cutaneous anthrax. Thousands of potentially exposed individuals were prescribed the antibiotic Cipro. The perpetrator is still unknown. This attack demonstrated that an individual could create highly refined anthrax spores, which, if disseminated properly, could infect hundreds, thousands or more. What is less clear is whether the perpetrator or any other terrorist could produce larger amounts (kgs) of anthrax and efficiently disseminate the spores over a wide area. According to the nuclear threat initiative, "Producing

kilograms of dried anthrax, which would be required for a mass-casualty attack against an urban target, would entail much greater technical difficulties and hazards."

Finally in 1984, a cult contaminated the salad bars at several restaurants in the Dalles, Oregon with the non-lethal bacterium Salmonella typhimurium. The cult's leaders used the event as a drill for sickening townspeople to prevent voter participation in an upcoming election. The cult's planner was an experienced nurse and microbiologist. Ma Anand Puja ordered antibiotic test kits containing salmonella bacteria from a laboratory supply company and used the cultures as seed organisms for the mixture cult members later sprinkled at the salad bars. Though there were public health and law enforcement investigations at the time, it was not until a cult member confessed that law enforcement realized the outbreak was the result of an attack. This illustrates the difficulty of differentiating naturally occurring and man made biological events. It also reinforces the fact that known perpetrators of biological and chemical attacks typically have some scientific training. Finally, it highlights the challenge posed by dual use equipment and materials.

In addition to these three major attacks, several incidences of minor food contamination and exposure to irritating substances make up the bulk of international chemical attacks in the MIPT database. For example, in 1978 several people attending an international Assyrian Congress meeting in Sydney Australia ate food contaminated with mustine hydrochloride. No group claimed responsibility, but Iraqi delegates provided the food to delegates who had criticized the Iraqi Government. As noted above mercury-contaminated fruit was found in several European countries in 1978, and in June 2003, at least seven letters containing the irritant Adamsite (a component of rocket fuel) were distributed across Belgium by an unknown group; in October and November 2003 envelopes containing ricin were intercepted in the mail system in the United States. In January 2003 two journalists who write on terrorism were attacked at a book signing in Greece by tear gas and red paint. In addition to the anthrax attacks in the United States, anthrax was also recovered from a letter sent to the Daily Jang Newspaper and a computer company both in Karachi in October 2001. No one was injured [41] and [4]. In December 2001, police vans in the Basques region of Spain were attacked with acid and Molotov cocktails — two were injured and no one claimed responsibility. In November 2001, tear gas was used to target a man in Bishkek Kyrgyzstan. There were no deaths and few injuries in any of these incidents, further bolstering the fact that motivational and technical challenges limit the destructive power of unconventional weapons.

6.2 Development and/or Attempted Use of CBRN

The number of unsuccessful attacks or even attempts at development or acquisition of CBRN far outweighs the actual use of these weapons. The dread and fear inspired by these weapons is even more unbalanced. The case of Aum Shinrikyo described above illustrates the difficulties encountered by a sophisticated terrorist organization trying to develop and deploy chemical and biological weapons. Aum also tried unsuccessfully to buy nuclear material weapons in Russia, even though it had approximately 30,000 members in the country at the time [Bunn 2005]. There is insufficient space to discuss all of the failed attempts in detail, but suffice it to say that al Qaeda and other relatively sophisticated groups, like Aum Shinrikyo, have, according to open sources, been unable to acquire the capability to use CBRN to mass effect, even though they continue to try.

There are a number of reasons for the absence of CBRN attacks including the technical and material challenges. In addition, while al Qaeda is set to destroy the West, few other groups have the motivation to kill large numbers of people. Other factors include: terrorists prefer the certainty of conventional weapons to the uncertainty of CBRN; the weapons can be hazardous to the terrorists themselves; the response to a CBRN terrorist attack may result in further degradation of terrorist capabilities; and finally political support of the terrorist organization's base may be turned away by the use of unconventional tactics.

While there have been few successful or large-scale CBRN attacks, experts clearly believe that attacks will be more sophisticated and occur more frequently in the future. Because the threat is difficult to predict policy makers have made tremendous investments in response and recovery efforts. One small part of this effort has been an investment in the science, technology and role of sensors.

7. Preventions Efforts — The Role of Sensors

What does all of this threat information mean for the design and deployment of sensors? Because of the infinite target spectrum described above, it is not only high value, highly secured 'targets' that must be monitored, but also softer, more common targets. Sensors must be able to find the proverbial 'needle in a haystack.' Because of the wide and varied threats, sensors would ideally be multifunctional, robust, low cost, accurate, reliable, used with little training, able to remotely discern signals in a high background environment, and would provide definitive information to decision makers and require little special care such as

refrigeration or power. According to the U.S. National Science Foundation, "It is essential to be able to accurately identify and measure in real time a wide range of chemical and biological agents, at levels much lower than toxic, in vapor and on surfaces, preferably from a distant position" [43].

7.1 What Are We Trying to Detect?

The U.S. spends an estimated $3.2 billion on research and development for combating terrorism, and John Marburger, the director of the Office of Science and Technology policy, noted that "A major role for technologies in combating terrorism is the detection of chemical, biological, radiological, nuclear, or conventional weapons of mass destruction [38]. Although the first part of this chapter is devoted to understanding the threat posed by terrorists, research and development of sensors for unconventional weapons, at least in the United States, has been more focused on worst-case scenarios than on the skills and motivations of the terrorists. As a result, many of the available sensors and sensors under development are designed to detect a specific subset of weaponized CBRN agents and not the non-lethal or unknown agents that may also be encountered. That being said, a short description of the high threat agents and materials that are the focus of United States government sensor research and development follows.

Biological Agents. Several U.S. Departments including Defense, Health and Human Services, Homeland Security, and Energy have been providing funding for biological sensors. The funding is directed to high priority threat agents as defined by the Centers for Disease Control and Prevention [15]. The threats are based on the ability to cause harm rather than demonstrated terrorist potential and are divided into Class A (high threat) and Class B (medium threat) biological agents. According to the CDC, Class A agents can be easily disseminated or are highly contagious, have high mortality rates, may cause public panic, and require special training and preparation. Class B agents are moderately easy to disseminate, have moderate or low morbidity, and require enhanced attention by CDC. Class A agents including Bacillus anthracis, the causative agent for anthrax; Clostridum botulinum toxin, which causes botulism; Yersinia pestis, the agent that causes plague; Variola major, which causes smallpox; Francisella tularensis, which causes tularemia; and Filo and arena viruses, which cause hemorrhagic fevers. Category B agents cause less serious disease and include food and water safety threats and Brucella species that cause brucellosis among others.

Chemical Agents. Sensors for chemical agents have focused mostly on known military chemical agents, which fall under six broad categories: blister agents, such as mustard, phosgene and lewisite; blood agents, such as cyanide; choking agents, such as phosgene and chlorine; incapacitating agents; nerve agents, such as Sarin and Soman; and riot control agents.

The U.S. government is also focused on the risk posed by attacks on industrial chemical facilities [53]. According to Massachusetts's representative, Edward Markey, "Chemical facilities are at the top of the terrorists' target list" [14]. However, because attacks on these facilities are more likely to result in a known release of a defined chemical entity, sensors are less important than situations where either the chemical release goes undetected or where an unknown substance is released.

Radiological Isotopes. Radioisotopes are in widespread daily use. Sources include the military, medical, industrial and academic communities. Until recently, radioisotopes were not strictly controlled. In the United States alone, there are approximately 22,000 licenses maintained by the Nuclear Regulatory Commission (NRC) and individual states through a special agreement with the NRC [60]. While a so-called dirty bomb is unlikely to cause significantly more casualties than a large bomb alone, policy makers are concerned with the public reaction following such an event. The primary contaminants are alpha and gamma emitters. As discussed above, national security experts deem a 'dirty bomb' as the most likely unconventional weapon over the next decade. As a result, effective detectors for the isotopes discussed below may be critical in alerting officials before an attack occurs or reducing health effects after an attack. For several isotopes, removing clothing after exposure can reduce the hazard by 90 percent.

Common radioactive material in use today includes: the alpha emitters Americium-241 and Plutonim-238; the beta emitters Phosporus-32 and Strontium-90; and the gamma emitters Cesium-137, Cobalt-60, and Iridium-192 [44]. These materials are commonly used in smoke detectors, oil exploration, industrial gauges, food and mail irradiation, cancer therapy, industrial radiography, and in research laboratories.

Nuclear Materials. The United States has deployed sensors both nationwide and overseas for the detection of nuclear materials. Although the presence of highly enriched uranium (an indication of a functional or potential nuclear weapon) would present the greatest threat, currently deployed sensors are unable to detect this material because of its low radioactivity. The Department of Homeland Security alone spent more

than $100 million in fiscal year 2004 to develop improved sensors for nuclear and radiological materials [17].

While nuclear materials are easier to track than CBR agents because of the complex facilities required to produce them, danger exists because several countries are reportedly diverting enriched materials from nuclear power plants, and because large stockpiles of fissile materials are not always sufficiently guarded. Terrorists have been unable to harness nuclear materials; however, between 1993 and 2004, according to the International Atomic Energy Agency, there were 650 documented instances of illegal transfers of nuclear and radiological materials [3]. In 2005, Russia's defense ministry reportedly prevented two terrorist attempts to infiltrate nuclear weapons sites [5]. The United States is working with Russia to increase the security of all nuclear stockpiles, yet much remains to be done [42]. Improved sensors are needed for fissile materials such as plutonium-239 and uranium-235, fussionable materials such as deuterium and tritium, and source materials such as tritium, polonium, beryllium, lithium-6 and helium-3.

7.2 Fielded Sensor Capabilities

Operational sensors are most effective at detecting substances in order to improve response — after the fact. Most detectors are not yet capable of providing warning. Once the presence of a potential hazard is detected by deployed sensors, more sophisticated instruments may be used — often off site — to further characterize the threat. Current sensors for chemical and biological agents use techniques such as ion mobility spectrometry, gas chromatography/mass spectrometry, blackbody infrared spectrometry, antibody kits, UV-induced fluorescence, and surface acoustic wave sensors [43]. Light detection and ranging systems (LIDAR) are being developed for remote detection. Some of these strategies are based on older technology due to the time it takes to fully field research. As a result they are often logistically difficult because they are large, expensive and require consumables as well as electricity and training [33].

Recognizing that nuclear materials are widely available and the terrorists' interests in radiological and nuclear devices, the United States Congress appropriated $300 million to the Department of Homeland Security to install radiation detectors at U.S. borders. Through 2005, DHS had installed 470 radiation portal monitors throughout the country including mail facilities and land and sea entries into the United States. The U.S. has also supported the installation of detectors at the borders of the states of the former Soviet Union through its Departments of State,

Energy and Defense. The General Accountability Office of the United States reported that currently deployed radiation detection equipment cannot sufficiently detect nuclear materials when they are shielded by lead or other metals, and that the equipment is least capable of detecting highly enriched uranium (HEU) because of the low relative radioactivity noted above. The detectors were also limited by the manner in which they were used [9]. For instance, to limit the number of false alarms from materials such as kitty litter and ceramics, border agents reportedly lowered the threshold sensitivity. The inspectors also allowed trucks to pass through monitors at rates of speed too high to efficiently detect radiation. The detectors were also adversely affected by environmental conditions such as wind, moisture and cold [3]. These deficiencies point to the need to improve sensor design.

The New York Times was even more unforgiving, "The federal government's efforts to prevent terrorist from smuggling a nuclear weapon into the United States are so poorly managed and reliant on ineffective equipment that the nation remains extremely vulnerable to a catastrophic attack" [36]. The newspaper reported that detectors at the Port Authority of New York and New Jersey suffer as many as 150 false alarms per day from 22 monitors, more than an order of magnitude greater than the predicted rate. Newly developed sensors must work quickly enough to facilitate the flow of goods and services across borders, and they must be both selective for and sensitive to low levels of radiation from materials of concern without a high rate of false alarms.

Biological. Biological detection is complicated by the fact that there are thousands of pathogens that might be used as biological weapons, and the means to detect microorganisms are often species specific. Current detection systems can be divided into three categories: environmental, hand-held mobile, and surveillance. All of the commercially available sensors are 'detect to respond' rather than 'detect to prevent' or warn. Environmental monitoring is generally defined as continuous or semi-continuous sampling of the environment in a fixed place. The U.S. Biowatch system is an environmental monitoring system dispersed nationwide in urban centers. It is designed to detect a biological event in 36 hours by filtering air at known time intervals, storing the samples, and amplifying the samples with polymerase chain reaction (PCR) twice if something is detected. Fluorescent-labeled probes for specific agents are introduced during PCR to allow detection of known threat agents. Some of the biggest challenges include understanding background concentrations of the agents being analyzed and sampling in a variety of different environmental backgrounds. Once a biohazard is detected, it

is sent to an approved laboratory for confirmatory testing. This type of system focuses on detecting known threats. Most mobile detectors are also pathogen specific. They are reduced in size and weight from the environmental samplers. Syndromic surveillance is also being used to detect attacks with biological pathogens. This involves the large-scale collection of health-related data that precede diagnosis but indicate the presence of an outbreak. (CDC, 2005)

Chemical. Exquisitely sensitive chemical agent sensors are available, but work best under laboratory conditions. Environmental chemical sensors suffer many of the same issues as biological detectors. They lack sensitivity, are not sufficiently mobile or flexible, and require trained users. Several types of chemical detectors are in use and are mentioned above.

Radiation. Radiation portal monitors have been in use for 20 years at U.S. nuclear facilities and are being used as part of the Second Line of Defense (SLD) program at Russian borders. At Los Angeles and Oakland ports, every container that is unloaded from a ship is screened before it leaves for its terrestrial destination and at other U.S. ports a portion of cargo is screened [7]. However, like the GAO, the National Institute of Standards and Technology in the United States recently evaluated 31 commercially available radiation detectors and found that most detectors could accurately measure gamma rays but not low energy x-rays [45]. Most current detectors were originally designed to be used under controlled conditions and not to detect terrorist events, where the instruments must be more flexible and detect a wider array of particles.

8. Improving Sensors

The research described in the remainder of this volume may advance the sensing of several of the materials listed above. To make radiation detectors useful for the detection of radiological materials and weapons, the instruments must be able to detect unknown types of radiation quickly, over a wide range of energies without delicate calibrations, and in many environments. In general, to improve sensor technology, sensors should address a wide variety of agents, be inexpensive, require little training to use and understand, be both accurate and reliable, be capable of withstanding extreme environments, require little or no power or reagents, be capable of remote detection and identification, and be able to discern signals in a high background environment regardless of environmental media.

9. Conclusions

While much of this chapter is focused on extreme Islamist terrorism, it should be emphasized that only a tiny fraction of the world's 1.44 billion Muslims support terrorism. Terrorism is a mindset and a tactic of extremes, either right or left, ethno nationalist, or religious. There has been much progress in the war on terrorism, but as demonstrated by recent attacks, we must remain vigilant for many reasons including:

1 Some of the most skilled and resolute terrorists remain at large including Osama Bin Laden, his deputy Ayman al-Zawahiri and Abu Musab al-Zarqawi,

2 Al Qaeda is resilient and has morphed from a more hierarchical group into a distributed organization, which will be even more difficult to defend against,

3 The war in Iraq has energized al Qaeda affiliates and other Islamic fundamentalist groups to fight the United States and other members of the coalition,

4 Regional organizations have also been impacted by the war on terrorism, but remain serious threats,

5 Cross-fertilization is increasing,

6 The spread of technology progresses onward, and it can be adapted for terrorist purposes.

Given the successes of the war on terrorism and the caveats listed above, research on sensors should address near term threats such as metals in weapons, explosives and improvised explosive devices (IEDs), and suicide packs, while continuing to address the longer-term threats of CBRN.

References

[1] Adnki.com, Indonesia: Jakarta Hotels on Full Alert, June 3, 2005, available at www.adnki.com/index_2level.php?cat+Terrorism&loid=8.0.173629318&par=0

[2] Aljazeera.net, "Full Transcript of bin Laden's Speech, " November 1, 2004, available at English.aljazeera.net.

[3] Aloise, Gene, "Combating Nuclear Smuggling: Efforts to Deploy Radiation Detection Equipment in the United States and Other Countries, June 21, 2005, GAO-05-840T.

[4] "Anthrax cases hit Pakistan," BBC News, November 2, 2001, available at news.Bbc.co.uk.

[5] "Army prevents terrorist attacks on nuclear sites," RBC, June 22, 2005, available at www.rbcnews.com.

[6] Associated Press, "Bin Laden tape: 'Youths of God' plan more attacks," October 7, 2002 accessed at http://www.smh.com.au/articles/2002/10/07/1033538881353.html, as cited in Gilmore 2002).

[7] Associated Press, "L.A. Port Getting Radiation Detectors," June 4, 2005, available at www.msnbc.msn.com/id/8092280.

[8] Associated Press, "Multiple Car Bombs Kill 23 in Baghdad," June 22, 2005, available at www.foxnews.com.

[9] Barrett, Devlin, "False Alarms Plague Port Anti-Nuke System," June 21, 2005, Associated Press, available at www.sfgate.com.

[10] Bolton, John R., Undersecretary of State For Arms Control and International Security, "The International Aspects of Terrorism And Weapons of Mass Destruction, "Second Global Conference On Nuclear, Bio/Chem Terrorism: Mitigation And Response, The Hudson Institute, Washington, DC Friday, November 1, 2002 as Released By The State Department and cited in Gilmore 2002.

[11] Bolton, John, R. "Iran's Continuing Pursuit of Weapons of Mass Destruction," Testimony before the House International Relations Committee Subcommittee on the Middle East and Central Asia, June 24, 2004, available at www.state.gov/t/us/rm/33909.htm.

[12] Bonner, Raymond, "Philippine Camps are training al Qaeda's Allies, Officials Say," New York Times, May 31, 2002 as cited in Gilmore 2002.

[13] Bunn, Matthew with Anthony Weir and Josh Freidman, "The Demand for Black Market Fissile Material," NTI, June 16, 2005, available at www.nti.org/e_Research/cnwm/threat/demand.asp.

[14] CBS News, "Chemical Threats Close to Cities," July 6, 2005, available at www.cbsnews.com/stories/2005/07/06/national/main706788.shtml.

[15] Centers for Disease Control And Prevention, "Syndromic Surveillance: an Applied Approach to Outbreak Detection," June 6, 2005 available at www.cdc.gov/epo/dphsi/syndromic.htm.

[16] A Chronology of Significant Terrorism for 2004, National Counterterrorism Center, United States, available at www. Fas.org/irp/threat/nctc2004.pdf.

[17] Department of Homeland Security, FY 2004 Budget Fact Sheet," October 1, 2003, available at www.dhs.gov/dhspublic/display?content=1817.

[18] DeSutter, Paula A. "U.S. Government Assistance to Libya in the Elimination of Its Weapons of Mass Destruction," Testimony before the Senate Foreign Relations Committee, February 2, 2004, available at www.state.gov/t/vc/rls/rm/2004/29945.htm.

[19] FBIS, "Russian Newspaper on Union of Islamic Movements in Central Asia," Moscow Pravda, September 16, 2002 as cited in Gilmore 2002.

[20] Finn, Peter and Dana Priest, "Weaker al Qaeda Shifts To Smaller-Scale Attacks," The Washington Post, October 15, 2002, http://www.washingtonpost.com/wp-dyn/articles/A25832-2002Oct14.html, as cited in Gilmore 2002.

[21] First Report to the President and Congress, 1999, The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, December 15, 1999, RAND.

[22] Fourth Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: Implementing the National Strategy, December 15, 2002, RAND.

[23] Freeh, Louis, "1999 Budget Request," testimony before the Senate Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies, March 3, 1998, available at www.fas.org/irp/congress/1998_hr/s980303f.htm.

[24] Gunaratna, Rohan, "The Future of Al Qaeda and the Islamist Terrorist Threat to Southeast Asia and Australia," Australian Security in the 21st Century, delivered at the Parliament House Canberra, May 27, 2003 available at www.mrcltd.org.au/uploaded_documents/thefutureofalqaeda.pdf.

[25] Higgins, Andrew, Karby Leggett, and Alan Cullison, "How al Qaeda put the Internet to use," The Wall Street Journal, November 11, 2002, http://www.msnbc.com/news/833533.asp?0si as cited in Gilmore 2002.

[26] Hinton, Henry L. testimony before the U.S. Senate Committee on Governmental Affairs, 17 October 2001, GAO-02-162T, p. 4 as cited in Gilmore 2002.

[27] Hoffman, Bruce, "Terrorism Trends and Prospects" Chapter Two in Countering the New Terrorism, Ian Lesser et al., 1999, RAND, MR-989-AF.

[28] Hoffman, Bruce, "RE-Thinking Terrorism in Light of a War on Terrorism," testimony before the subcommittee on Terrorism and Homeland Security, House Permanent Select Committee on Intelligence, U.S. House of Representatives, September 26, 2001, available at www.rand.org/publications/CT/CT182?CT182.pdf.

[29] Hoffman, Bruce, "Al Qaeda, Trends in Terrorism And Future Potentialities: An Assessment," 2003, RAND P-8078.

[30] Jarboe, James F., FBI, "The Threat of Eco-Terrorism," testimony before the House Resources Committee, Subcommittee on Forests and Forest Health, February 12, 2002, available at www.fbi.gov/congress/congress02/jarboe021202.htm.

[31] Jenkins, Brian M., "The Future Course of International Terrorism," The Futurist, July–August, 1987, available at www.wfs.org/jenkins.htm.

[32] Jenkins, Brian M. "The Organization Men: Anatomy of a Terrorist Attack," in James F. Hoge, Jr. and Gideon Rose, How Did This Happen? Terrorism and the New War (NY: Public Affairs, 2001).

[33] Kosal, Margaret, "The Basics of Chemical and Biological Weapons Detectors", November 24, 2004, Monterey Institute of internationals Studies, available at cns.miis.edu/pubs/week/031124.htm.

[34] Kyodo News Service, Japan, "Aum Shinrikyo Sets Up More Than 10 Business Entities" April 16, 2004, available at www.religion newsblog.com/6796.

[35] Lake, Eli, "Al Qaeda's Disinformation War," October 30, 2002, The New Republic Online.

[36] . Lipton, Eric, "U.S. Borders Vulnerable, Witnesses Say," June 22, 2005, New York Times.

[37] Lugar, Richard, "The Lugar Survey on Proliferation Threats and Responses," June 2005, United States Senator For Indiana, Chairman Senate Foreign Relations Committee.

[38] Marburger, John, Statement before the subcommittee on emerging threats and capabilities committee on armed services, United States Senate, April 10, 2002, available at armed-services.senate.gov/statement/2002/April/Marburger.pdf.

[39] Marshall, Andrew, "It Gassed the Tokyo Subway, Microwaved Its Enemies and Tortured Its Members. So Why is the Aum Cult Thriving?" The Guardian, July 15, 1999.

[40] The MIPT Terrorism Annual 2002, with contributions from D. Brannan, P. Chalk, K. Cragin, and S. Daly, National Memorial Institute for the Prevention of Terrorism, available at www.mipt.org.

[41] MIPT Terrorism Knowledge Database, available at www.tkb.org.

[42] National Academy of Sciences, Making the Nation Safer: the Role of Science and Technology in Countering Terrorism, 2002.

[43] "The New Challenges of Chemical and Biological Sensing: National Science Foundation Workshop," January 9-10, 2002, Arlington Virginia, available at www.chemistry.gatech.edy/sensing forum-02/welcome.html.

[44] News & Terrorism: Communicating in a Crisis, Fact Sheet from the National Academies and the Department of Homeland Security, Radiological attack: Dirty Bomb and Other Devices, available at nae.edu/NAR/pubundcom.nsf/weblinks/CGOZ-646NVG/$file/radiological%20attack.pdf.

[45] Pappalardo, Joe, "Security Beat," National Defense, July 2005 available at www.nationaldefensemagazine.org/issues/2005/jul/security_Beat.htm.

[46] Patterns of Global Terrorism 2001, Office of the Coordinator for Counterterrorism, U.S. State Department, May, 2002 available at www.state.gov/s/ct/rls/pgtpt/2001.

[47] Patterns of Global Terrorism 2003, Office of the Coordinator for Counterterrorism, U.S. State Department, April 29, 2004 available at www.state.gov/s/ct/rls/pgtpt/2003/31644.htm.

[48] Perl, Raphael, "Terrorism and National Security Trends," CRS Issue Brief for Congress, December 21, 2004, available at www.fas.org/irp/crs/IB10119.pdf.

[49] Raman, B., "The LTTE: The Metamorphosis," Paper no. 448, South Asia Analysis Group, April 29, 2002 available at 222.saag.org/papers5/paper448.html.

[50] Raman B., "The World's First Terrorist Air Force," Observer Research Foundation, available at www.observerindia.com/analsysis/A445.htm.

[51] Shannon, Elaine, "Another warning from Zubaydah," Time, May 11, 2002, http://www.time.com/time/nation/article/0,8599,236992,00.html, as cited in Gilmore, 2002.

[52] Smith, G. Davidson, Combating Terrorism, London, Routledge, 1990, p. 7 as cited in G. Davidson Smith, "Single Issue Terrorism," Commentary No. 74, Canadian Security Intelligence Service, Winter 1998, available at www.csis-scrs.gc.ca/eng/comment/com74_e.html

[53] Stephenson, John B., "Homeland Security: Federal and Industry Efforts are Addressing Security Issues at Chemical Facilities, but Additional Action is Needed," April 27, 2005, GAO-05-631T.

[54] "Summary of Investigation of IRA Links to FAC Narco Terrorists in Colombia," Majority Staff of the U.S. House International Relations Committee, April 24, 2002, available at wwwa.house.gov/international_Relations/107/findings.htm.

[55] Swartz, Jon, "Terrorists' Use of Internet Spreads," USAToday, February 20, 2005, available at www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-usat_x.htm.

[56] Tenet, George, Director of Central Intelligence, "The Worldwide Threat 2004: Challenges in a Changing Global Context," testimony before the Senate Select Committee on Intelligence, February 24, 2004.

[57] Terrorism: Questions and Answers: North Korea, Council on Foreign Relations, 2004, available at cfrterrorism.org/sponsors/northkorea.html.

[58] Terrorism: Questions and Answers: Syria, Council on Foreign Relations, 2004, available at cfrterrorism.org/sponsors/northkorea.html.

[59] United States District Court, District Court of Massachusetts, United States of America v. Richard Colvin Reid, http://news.findlaw.com/hdocs/docs/terrorism/usreid011602ind.html, as cited in Gilmore 2002.

[60] U.S. Nuclear Regulatory Commission, The Regulation and Use of Isotopes in Today's World, available at www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0217/r1/br0217r1.pdf.

[61] Williams, Mike "Analysis: What next for al Qaeda?" November 22, 2001, http://news.bbc.co.uk/1/hi/world/south_asia/1678467.stm, as cited in Gilmore 2002.

[62] Zakis, Jeremy and Steve Macko, "Major Terrorist Plot in Singapore Discovered: al Qaeda Believed well Established in the Asian Region", January 12, 2002 available at www.emergency.com/2002/jamaah_islamiyah.htm as cited in Gilmore 2002.