Terrorism Risk in the Post-9/11 Era

A 10-Year Retrospective

■ FOREWORD

Rendering of the 9/11 Memorial, located at the site of the former World Trade Center, New York City.

The September 11, 2001 terrorist attacks shocked the world—the scale of loss inflicted by this tragedy still elicits a visceral reaction today. My colleagues and I witnessed firsthand the devastation in the wake of 9/11, as we had visited clients in the World Trade Center just the previous day. Alongside so many others in New York City, we spent the following days coming to grips with the consequences of the attack, and its implications for the rest of the world. These tragic events forever changed the U.S. threat landscape, and the world's understanding of terrorism risk.

A decade later, the day's events still impact us on many levels, from our increased awareness of the threat in our daily lives, to the heightened security measures, known and unknown, that protect us. Recognition that terrorism threat can range from the macro to the micro scale has changed how homeland security forces think about interdiction, and the way in which governments, businesses, and the insurance industry, manage potential terrorism loss.

On this 10-year anniversary, we at RMS take the time to reflect, not only on the political and sociological implications of a decade of terrorist threat, but on the transformative impact of the event on the insurance industry. The "game theory" engine that helps formulate the probabilities of successful terrorist attacks was conceptualized by Dr. Gordon Woo at RMS, and has helped to shape the way our clients and others think about terrorism risk. The targeting and attack mode likelihoods and characteristics modeled from game theory based-analysis of the adversary have proven highly consistent with the characteristics of successful attacks and plot attempts.

The threat of terrorism stays with us, despite the mobilization of an alliance of Western nations to eliminate it at the source, and it is the unfortunate reality that this threat will continue in some form for years to come. The Western security and counterterrorism intelligence shield has proven vital in keeping the attack frequency low in the U.S. and Europe. In other countries, terrorism rages with less interdiction success, and more than 25,000 people worldwide are estimated to have died in militant Islamic terrorist attacks since 9/11.

RMS is proud to have been part of the thought leadership in helping our clients adjust to managing this new risk landscape into the future. Beyond the insurance sector, RMS expertise has been used in government reports and cited in Congressional hearings, and contributed to the conceptualization and U.S. Treasury costing of the Terrorism Risk Insurance Act. As part of the industry's engagement in policy-making, RMS co-founded the RAND Center for Terrorism Risk Management Policy, which conducted independent terrorism research and published public policy reports.

While we look forward with hope backed by greater assurance that a recurrence of the tragic events of 9/11 is unlikely, the threat remains; and we are committed to supporting our clients and stakeholders, as we have over past 10 years, in understanding and managing this risk.

Hemant Shah

Hemant Shah
President and CEO
RMS

■ TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

In the decade since the tragic events of September 11, 2011 (henceforth referred to as the 9/11 attacks), the understanding and management of terrorism risk has forever changed. In "Terrorism Risk in the Post-9/11 Era: A 10-Year Retrospective," RMS' terrorism modeling experts share their analysis and perspectives on the evolution of the terrorism threat, its impact on the insurance industry, and the future of terrorism risk; and discuss the tools and best practices that help insurers manage this risk.

Analyzing Terrorism Risk

Terrorism risk analysis assesses the likelihood that a successful terrorist attack will occur, and estimates the loss that such an attack would subsequently cause. This risk can be broken down into three main components:
- The threat, which is a function of the group's intent and capability
- The target's vulnerability to the threat, which is a function of the counterterrorism landscape
- The consequences resulting from a successful attack
  The six chapters in this report address these components in the context of the 9/11 attacks and their impacts on the evolution and future of terrorism risk.

The Post-9/11 Global Terrorism Landscape

The 9/11 attacks heralded a new era of global terrorism marked by Al-Qaeda and its affiliates exhibiting an increased ambition in the scale of attack and in their determination to inflict maximum casualties. This chapter reviews the evolution of the global terrorism landscape since 9/11 by analyzing terrorism patterns, themes, and trends. It concludes with an assessment of how the global terrorism landscape may look in the future.

Evaluating the Al-Qaeda Threat to the U.S. Since 9/11

Since the 9/11 attacks, Al-Qaeda has become the most hunted terrorist organization in the world. The group has lost many of its key senior members, including iconic leader Osama bin Laden; a number of Al-Qaeda affiliates have been substantially weakened; and a series of ideological challenges have confronted the group. Despite these offensive strikes, it is too early to declare the terrorism threat from Al-Qaeda and its affiliates to be over. The groups remain resilient and intent on attacking the U.S. This chapter reviews the current threat to the U.S. from the Al-Qaeda core as well as emergent homegrown jihadi and other groups, and how the U.S. terrorism landscape has evolved since 9/11.

The Post-9/11 U.S. Counterterrorism Landscape

The U.S. response to 9/11 has been broad-based, with massive counterterrorism initiatives undertaken to reshape U.S. domestic law enforcement and intelligence agencies to provide better and stronger security. This chapter provides an overview of U.S. homeland security initiatives, and assesses how the U.S. counterterrorism landscape may change in the future.

Evaluating Al-Qaeda's Post-9/11 CBRN Capabilities

Chemical, biological, radiological, and nuclear (CBRN) weapons attacks constitute a sizeable portion of the terrorism risk confronting the insurance industry. A CBRN attack is most likely to occur in a commercial business center, potentially generating significant business interruption losses due to evacuation and decontamination, in addition to any property damage or casualties that occur. This threat has become a growing concern, as there is strong evidence that Al-Qaeda and its affiliates are interested in acquiring a CBRN agent to execute a mass casualty event. But, does intent equate with capability? This chapter reviews Al-Qaeda's CBRN development efforts in the last decade, and discusses the probability of Al-Qaeda launching a successful attack today.

Modeling Terrorism Frequency

One of the most contentious components of terrorism risk modeling is the estimation of attack frequency. Many risk managers consider models incapable of estimating the number of major terrorist attacks in any given period of time, as human actions are impossible to forecast. RMS considers frequency modeling to be not only possible, but necessary for managing terrorism risk. This chapter explores this concept and its underlying methodology to illustrate how frequency estimates can be robustly modeled.

Quantifying and Managing Terrorism Risk

Over the last decade, insurers and reinsurers have used many analytical tools to manage and underwrite terrorism risk. This chapter reviews the evolution of terrorism risk management and offers insight on how approaches to underwriting and managing terrorism risk have evolved since the 9/11 attacks, and discusses best practices for managing terrorism risk. The chapter concludes with RMS' perspective on how the market will manage this risk in the future. ■

2 THE POST-9/11 GLOBAL TERRORISM LANDSCAPE

A decade after the 9/11 attacks on the U.S., this seminal event continues to reverberate around the globe. Despite efforts from the global community, terrorism remains the preeminent security threat. Al-Qaeda and its affiliated groups remain active and have orchestrated a number of attacks worldwide. This chapter reviews how the global terrorism landscape has evolved in the post-9/11 environment by analyzing terrorism patterns, themes, and trends, and concludes with an assessment of how the global terrorism landscape may look in the future.

A Pivotal Decade in Terrorism History

The sheer scale and magnitude of the 9/11 attacks, executed by a network of individuals intent on producing a simultaneous mass-casualty event, stunned the world and moved the threat of terrorism to the forefront of many countries' security priorities. In addition to causing significant loss of life and physical destruction, the attacks also resulted in one of the most costly insurance events in the history of the United States.

The past decade's events, from the attacks themselves to the ensuing "Global War on Terror," have molded the current global terrorism landscape. Against the backdrop of these conflicts, events such as the Mohammed cartoon controversy, the problems related to the existence of Guantanamo Bay, the Abu Ghraib scandal, and the outrage following the ban of the *niqab* (face cover) in

several Western European countries have helped to fuel the narrative of the global Salafi-jihadi movement, causing an increase of recruits to Al-Qaeda and its affiliated groups.[1]

The threat from the Salafi-jihadists has also shifted dramatically over the last ten years. Al-Qaeda's core organization suffered a number of setbacks, from the loss of senior members, including iconic leader Osama bin Laden, to the destruction of several important training facilities. However, the group has consistently shown the ability to reorganize and resume planning and directing attacks. Since 9/11, Al-Qaeda has abetted a process of global radicalization that has motivated, inspired, and created independent terrorist cells and groups. Using Al-Qaeda connected websites such as Al-Sahab, the jihadist movement has helped to radicalize Muslims across the globe. Globally, successful or foiled terrorism plots such as the 2006 attempt by jihadists to detonate liquid explosives carried on board at least 10 transatlantic airliners traveling from the U.K. to U.S. continue to serve as a somber reminder of the threat from Salafi-jihadists.

These plots and attacks have helped to make the last decade one of the most active in terrorism history. According to RMS' historical catalog of macro terrorism attacks (defined as attacks with the minimum severity of

## The Post-9/11 Rise of Salafi-Jihadism

Salafi-jihadism is a revivalist Islamic movement that seeks to recreate the true Islamic community and way of life. The Salafi-jihadi movement is broken down into a hierarchal structure with the Al-Qaeda core on top, affiliate groups in the middle, and homegrown jihadi groups at the bottom. Framing its cause as a defensive jihad to protect the Muslim population, the group's leaders create a narrative that resonates within the Salafi-jihadi community, motivating them to take up arms to fight for their mission.

The rise of Salafi-jihadi groups has significant implications for the global terrorism landscape. Religiously oriented groups tend to be more rigid, violent, and less willing to negotiate, in part because they view their conflict in a binary fashion of good against evil. These groups also present a greater threat given their higher proclivity toward mass casualty attacks relative to their secular counterparts. The

resurgence of this type of terrorism on such a violent scale over the last decade is unprecedented and will remain the most dangerous category of terrorist groups for the foreseeable future.

Composition of the Salafi-Jihadi Threat

- Al-Qaeda Core
- Affiliated Groups
- Independent Operatives
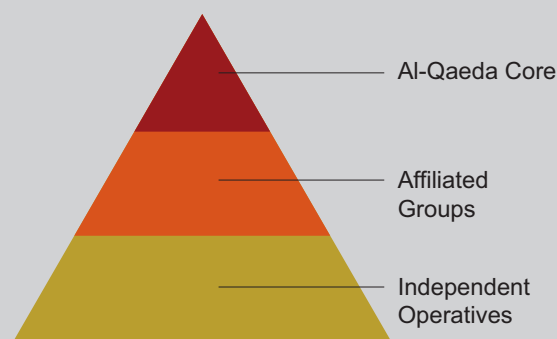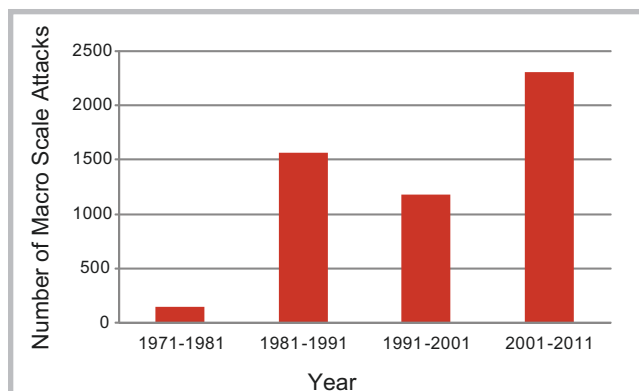
The number of macro terrorism attacks worldwide, by decade, since 1970.[3]

a car bomb) terrorist violence has increased substantially since 9/11.[2] More than 2,400 macro attacks have occurred worldwide since 2001, killing over 37,000 people and injuring nearly 70,000. More than 60% of these victims have been in Afghanistan and Iraq. Levels of terrorist violence that would have been considered excessive prior to 9/11 have become the norm and while there are signs of the attack tempo abating, the magnitude and frequency of events remain high compared to previous decades.

While the West has suffered relatively few major terrorist attacks, those that have succeeded show that Western defenses can still be vulnerable. For example, the March 11, 2004 Madrid commuter train bombings by terrorists inspired by Al-Qaeda killed nearly 200 people and wounded 1,800. And, on the morning of July 7, 2005, four suicide bombers successfully detonated bombs on the London Underground, killing 52 people and injuring over 700. Even failed terror attacks are regarded as successes by Al-Qaeda because of the reaction they provoke from those targeted. Such attacks serve to create a sense of insecurity among the general population, and have required a significant investment in both financial as well as human resources, threatening to bleed Western economies during this time of economic austerity.

The Rise in Religious Terrorism

Since 9/11, the frequency, magnitude, and scale of terrorist violence motivated by religion has increased, as has its global reach. Religious terrorism is founded in the belief that a celestial power has sanctioned terrorist violence for the greater glory of the faith, and therefore acts committed in the name of the faith will be forgiven by this divine power.[4]

In the last decade, more than 92% of all macro terrorist attacks have been linked to religious terrorist organizations. Macro terrorist attacks from ethno-nationalist, ideological, and separatist groups such as the

Euskadi Ta Askatasuna (ETA), Liberation Tigers of Tamil Eelam (LTTE), Abu Nidal Organization (ANO), and the Japanese Red Army (JRA)—the dominant terrorist forces for the last two to three decades—have sharply declined. Their ideologies of class conflict, colonial liberation, and secular nationalism have been challenged by a new and vigorous infusion of religious philosophies.

Within the realm of religious terrorism, militant groups linked to the Al-Qaeda-led Salafi-jihadi domain have been the most active.

Far and Near Enemies

Since 9/11, macro terrorism attacks have been committed in more than 40 countries worldwide. While the Middle East and South Asia are still the epicenter of the threat, terrorist attacks extend far beyond these regions. This dispersion of threat is largely credited to the activities of Al-Qaeda and its affiliates within the Salafi-jihadi movement.

Salafi-jihadi strategists have long debated whether they should focus their efforts on the West, dubbed "the far enemy," or whether they should first attack their own apostate regimes, "the near enemy." From the 1980s onward, jihadi discourse was dominated by those who believed that attacks on the apostate regime were a priority. However, with the 9/11 attacks, Osama bin Laden spearheaded the concept that countries in the Middle East can only be liberated by an attack on the far enemy—the United States.[5]

Since the invasion of Afghanistan and Iraq, Salafi-jihadi strategists have argued for a hybrid approach by incorporating both far and near enemies within their target calculus. The presence of Western troops and the host governments they protect has created further opportunity and incentive for jihadists to attack the "near" areas with the purpose of first driving the Western presence out of the region to then focus on the apostate regime. This hybrid strategy does not preclude attacks on "far" areas and Al-Qaeda will strike on Western soil if it will further its goals and the opportunity is at hand.[6]

One manifestation of this approach is evident in the Western European plots by groups linked to or inspired by Al-Qaeda. Though no successful macro attacks have taken place in Western Europe since the July 2007 attacks in London, an extensive number of plots have been disrupted by European security agencies. According to RMS research, since 9/11, Salafi-jihadis linked to Al-Qaeda have prepared an average of four macro plots per year in Western Europe.

The most at-risk Western European countries today are the U.K., Spain, France, Germany, Italy, and Denmark These countries have been targeted by Salafi-jihadi groups

due to their policies and practices, as demonstrated by the outrage within the Salafi-jihadi community toward the publication of cartoons deemed offensive to the prophet Mohammed in a Danish newspaper.[7] National foreign policies have become important considerations as well. This has been particularly true of military actions overseas in Muslim countries and more so for former colonial powers such as France and the United Kingdom.[8]

When viewed in the context of Europe's history of political violence, religious terrorism, particularly the Salafi-jihadi variant, could be considered a marginal phenomenon. Yet, empirical data suggests that it constitutes an ever-growing and increasing threat. It is also a troubling trend in the context of heightened tensions between the Muslim world and the West in light of the 9/11 attacks as well as the Western military incursions in Afghanistan and Iraq.[9]

The Move Toward Smaller Bombs

Mass casualty attacks are still the intention of groups within the Salafi-jihadi movement, and the 9/11 attacks raised the expectations of what represents a large-scale attack. Nevertheless, while the conviction to attack in the Salafi-jihadi community remains strong, ultimately, threat is measured by both intent and capability. The

Average Macro Terrorism Plot Frequency

- High (>4)
-
-
-
- Low (<1)

Relative frequency of terrorism plots in Western Europe since 9/11.

group's capability to implement a large-scale attack, particularly in the West, where the counterterrorism environment is much more robust, is currently far less impressive than it was a decade ago.

These limited capabilities have resulted in a move by Al-Qaeda and other groups to use smaller bombs for attacks. Of the almost 2,000 vehicle bombs detonated by terrorists worldwide since 2001, the largest yield has been around 2 tons TNT-equivalent (about the size of the 1995 Oklahoma City bombing in the U.S.). This has occurred even where munitions are freely available in conflict zones like Afghanistan and Iraq. Thus, it is not a short supply of explosives but the heightened counterterrorism environment that has impeded these groups from using larger attack modes.

While the types of technology used have not substantially changed, the methods terrorists use to deploy their conventional weapons have evolved significantly. Attacks today occur in densely populated areas, at a time of day selected to cause the most damage and fatalities. By refining their targeting and timing, terrorists have become more efficient, making major impacts with lesser-yield bombs.

Focusing on Soft Targets

Since the 9/11 attacks, target "hardening" of government buildings by national security agencies has forced terrorist groups to focus on "softer" commercial and economic targets. Hotels and other economic and business entities are key targets, since many jihadi groups lack the ability to attack more secure targets such as government buildings, embassies, and military bases.

Commercial targets such as hotels are at the greatest risk. According to a report from the global security consultancy Stratfor, the number of hotel attacks has more than doubled in the decade since 9/11 compared to the decade before.[10] Injuries and deaths caused by those attacks have increased six times over the same comparison period.[11] Hotels are ideal targets, as these locations must remain open to the public, making it difficult to identify and exclude those with hostile intentions.

As illustrated by the Madrid train and London Underground bombings, transportation infrastructure is also a key target due to the high density of people, its public nature, and the disruptive impact of an attack on the flow of transportation.

Also emerging in the post-9/11 environment has been Al-Qaeda's strategic focus on Jewish and Christian targets.[12] Places of worship are targeted by terrorist groups such as Al-Qaeda because of their view that their jihad is between the Muslims on one side and Christians
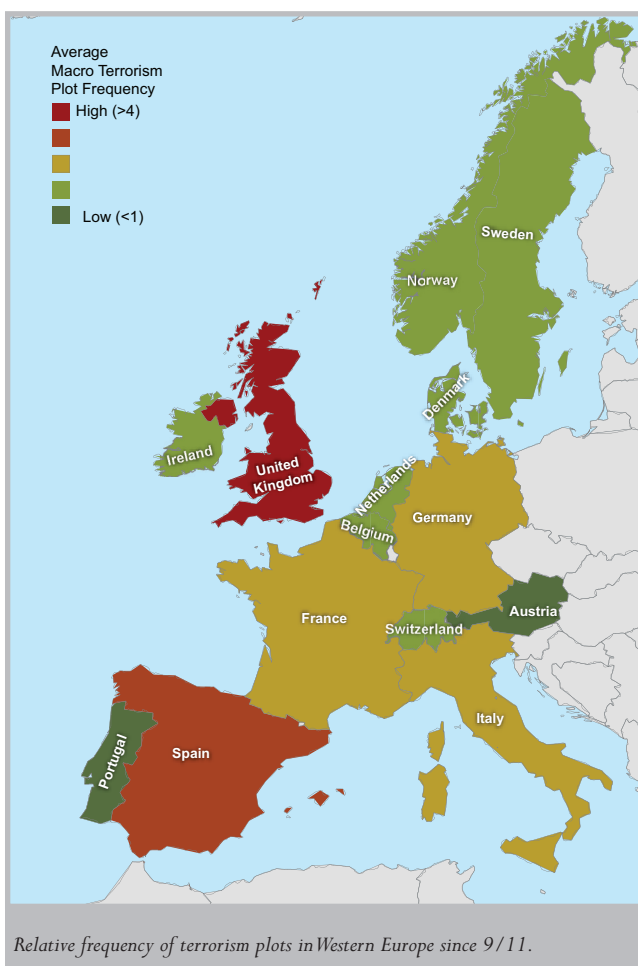
Al-Qaeda has focused on synagogues and Jewish community centers as terrorism targets in the decade since 9/11.

and Jews on the other. Churches and synagogues are the most at risk, as there are perceptions within Al-Qaeda and its affiliates that the people involved with these sites are proselytizing.

Al-Qaeda and its affiliate groups began to focus their resources on Jewish and Israeli targets after 2002, bombing synagogues and Jewish centers in Tunisia, Morocco, and Turkey, and attacking an Israeli-owned hotel in Mombasa, Kenya. Al-Qaeda's North African affiliate also orchestrated an attack at the Israeli embassy in Mauritania in 2008.

The Future Terrorism Landscape

Projecting future trends in global terrorism is a challenge because the threat of terrorism is highly dynamic, and is a function of the geopolitical landscape at any given juncture. However, current factors indicate that the strength of the Salafi-jihadi movement could soon wane. The failure of the movement to deliver any observable improvements to the lives of its would-be constituents in the last decade makes such a decline a distinct possibility. The democratic uprising that has been sweeping through the Middle East has eroded Al-Qaeda's ideological standing among its supporters. Moreover, the death of Osama bin Laden represents both a symbolic and strategic loss due to his status within the Salafi-jihadi movement.

Even so, Al-Qaeda and its affiliates are highly resilient and adaptive, and underestimating their abilities would be dangerous. The death of Osama bin Laden, while a blow to the global Salafi-jihadi movement, does not impede its operational trajectory. The political upheaval in the Middle East also does not completely undermine the cause of Al-Qaeda and its affiliates. The Salafi-jihadi ideological premise is not limited to the political grievances prevalent in the Middle East, but also draws

on conflicts in Afghanistan, Chechnya, Kashmir, Somalia, and beyond. Thus, while the future global terrorism landscape is uncertain, the Salafi-jihadi threat is likely to remain a lasting presence for the foreseeable future. ■

Notes and References

1. Coburn, Andrew & Woo, Gordon, "How Did the Terror Risk Models Stack Up?" Risk & Insurance Online, September 15, 2008, http://www.riskandinsurance.com/story.jsp?storyId=126852518, (accessed on June 2, 2011).

2. RMS defines macro terrorism attacks as those capable of causing (1) economic losses in excess of $1 billion; (2) more than 100 fatalities or 500 injuries; or (3) massively symbolic damage.

3. Source: RMS Terrorism Catalog & National Consortium for the Study of Terrorism and Responses to Terrorism's (START) Global Terrorism Database (GTD).

4. Rapoport, David, "Sacred Terror: A Contemporary Example from Islam," in Walter Reich (eds) Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind, Woodrow Wilson Center Press, 1998, Pg. 110.

5. Brooke, Steven, "Strategic Fissures: The Near and Far Enemy Debate," Assaf Moghadam and Brian Fishman (eds) "Self Inflicted Wound, Debates and Divisions within Al-Qaeda and its periphery," Combating Terrorism Center at West Point, December 10, 2006, Pg. 50.

6. Ibid, Pg. 52.

7. Pillar, Paul, "The Diffusion Of Terrorism" Mediterranean Quarterly - Volume 21, Number 1, Winter 2010, Pg. 10.

8. Ibid.

9. Benjamin, Daniel & Simon, Steven, "The Next Attack: The Failure of the War on Terror and a Strategy for Getting it Right, "Times Book, 31 October 2005, Pg, 220.

10. "Special Security Report: The Militant Threat to Hotels," Stratfor, September 8, 2009, www2.stratfor.com/…/20090901_security_militant_threat_hotels, (accessed on June 2, 2011).

11. Ibid.

12. Bergen, Peter & Hoffman, Bruce, "Assessing the Terrorist Threat: A Report of the Bipartisan Policy Center's National Security Preparedness Group" Bipartisan Policy Center, September 10, 2010., Pg 30.

The Death of Osama bin Laden and Its Implications for Future Terrorism Risk

The assassination of Osama bin Laden caused a major blow to the global Salafi-jihadist movement. Others in the movement might have the operational and tactical expertise to launch macro attacks, but bin Laden's charisma and organizational skills incited Al-Qaeda and its affiliated groups to launch attacks across the globe. Osama bin Laden had hoped that his life would inspire like-minded Salafi-jihadists to follow his lead. And, in death, bin Laden has indeed become a martyr for his followers. Nevertheless, his demise leaves a significant leadership hole in the Al-Qaeda network, lessening the potency of the movement.

Bin Laden's death adversely affects the ideological cohesion of the disparate groups within the global Salafist movement; but does not end the threat from Al-Qaeda and its affiliates for three primary reasons. First, bin Laden's death does not affect the core operational structure of Al-Qaeda, as other senior stewards of Al-Qaeda such as its new leader, Ayman Zawahiri, and its key military commander, Saif Adel, have already assumed operational control. Second, the Al-Qaeda of today is much less hierarchical and more highly diffused than the organization bin Laden created in 1988. Currently, the main threat to the U.S. and other Western countries comes from regional affiliates of Al-Qaeda in Afghanistan, Iraq, Pakistan, and Yemen, as well as homegrown groups in Western countries. All have pledged allegiance to Al-Qaeda, but each has the autonomy to operate on its own discretion. Third, within the ideological space, bin Laden had already been playing a less prominent role in the last few years. The mantle for the Al-Qaeda ideology has been taken up by Ayman Zawahri and, more significantly, by Anwar Awlaki, an American citizen who has become a senior leader of Al-Qaeda in the Arabian Peninsula.

The appointment of Zawahiri to replace bin Laden as the leader of Al-Qaeda, while not unexpected, has many counterterrorism experts skeptical of its efficacy. Zawahiri's background seems ideal for an aspiring terrorist leader. He is a highly intelligent Egyptian radical Islamist and a key strategist within the global Salafi-jihadi circles. Nevertheless, his reputation as a divisive figure and a poor orator compared to bin Laden makes it difficult for members of Al-Qaeda to rally behind him; particularly when the Al-Qaeda core is under constant threat from U.S. counterterrorism efforts.

In the near term, reprisal attacks across the globe in retaliation for bin Laden's death are expected. These attacks are intended to demonstrate that the Al-Qaeda movement remains operational and intact. Terrorism plots against U.S. and Western installations such as embassies and military barracks in high terrorism risk areas such as in Afghanistan, Iraq, Pakistan, Somalia, and Yemen should be expected. However, in the West, particularly in the United States, major terrorism plots are unlikely, as such attacks will take time to organize and execute. Terrorist groups such as Al-Qaeda are meticulous. They are patient and will wait for security to be lowered before mounting a major attack. With the heightened security in place following bin Laden's demise, it is unlikely that a terrorist group or an individual operative will be able to orchestrate a large attack in a Western country.

Over a longer time horizon, we need to be cognizant that Osama bin Laden was just one component of the global Salafist movement, albeit a large one. The real strength of Al-Qaeda has never been its global infrastructure or its leadership per se, but rather its overarching ideology. As long as the ideology remains intact, the movement will be able to resuscitate itself. Unfortunately, the political oxygen needed to fuel the cause remains abundant. Al-Qaeda is still able to leverage injustices resulting from conflicts in Afghanistan, Chechnya, Iraq, Kashmir, Somalia, and beyond to draw recruits. Thus, in the long run, to quell the terrorism threat from Al-Qaeda, it is essential not only to remove terrorism's operational space by killing key leaders such as Osama bin Laden, but it is imperative that the ideology be discredited as well. Until this is accomplished, the long-term terrorism threat landscape will remain much the same.

Osama bin Laden

EVALUATING THE AL-QAEDA THREAT TO THE U.S. SINCE 9/11

A decade after the 9/11 terrorist attacks, Al-Qaeda and its affiliated groups continue to pose a significant security threat to the United States. Although an attack of similar magnitude to what transpired in 2001 appears unlikely, Al-Qaeda and its affiliates continue to have the intention as well as the capacity to launch a significant terrorist attack in America. This chapter reviews Al-Qaeda's present threat to the U.S. homeland, and examines how the terrorism landscape has evolved since the 9/11 attacks, including the rise of homegrown jihadi terrorists and affiliated groups.

THE AL-QAEDA THREAT IN THE UNITED STATES

The threat from Al-Qaeda to the U.S. remains elevated. In the decade since 9/11, U.S. foreign policy strategy, particularly the military intervention and occupation of Afghanistan and Iraq, has placed the U.S. and its interests at greater peril. The U.S. military presence in Iraq has alienated many in the global Muslim community and has increased the ranks of individuals willing to be recruited by Al-Qaeda to wage attacks against the United States. While the death of Osama bin Laden is a major blow to its cause, Al-Qaeda's ideological aim is to invigorate the global jihad movement by exploiting the widespread suffering and resentment evoked by such events.

According to RMS research, since 2002 nearly 40 plots inspired by or connected to Al-Qaeda have occurred in the United States. From 2002–2008, the number of plots declined; but from 2008 onward, the number of attacks perpetuated by groups or individuals linked to Al-Qaeda has been on the rise. While the lethality of these plots has been relatively low and the perpetrators were often amateurs who displayed more enthusiasm than skill, this increase indicates that the threat landscape has yet to improve.

The Al-Qaeda threat within the U.S. has also become much more diverse. In the early years after 9/11, the

primary concern within the U.S. counterterrorism community was the risk of an attack on the U.S. homeland from Al-Qaeda core leadership. As time passed however, this threat broadened to include individuals unaffiliated with but inspired by Al-Qaeda to engage in terrorist attacks, as well as Al-Qaeda core senior operatives assigned to strike against American targets.

ROLE OF THE AL-QAEDA CORE

Because the Al-Qaeda core's operational space has been greatly reduced due to the robust counterterrorism environment in the United States, it is unlikely that the group could mount an attack similar to what transpired on 9/11. Nevertheless, Al-Qaeda has accused the U.S. of actively attacking Muslims, and thus its intent to retaliate will remain even if the opportunity to do so jeopardizes its own security. Al-Qaeda senior leaders in Pakistan have been identifying, training, and placing operatives in the U.S. to conduct simpler but still deadly attacks. Najibullah Zazi's plot against New York City's subway system in September 2009 is just one example.

Moreover, the Al-Qaeda core has always strategically asserted its role beyond the operational prism, and continues to provide ideological direction and inspiration to its supporters. Since 2002, the presence of American troops in Afghanistan and Iraq has been used by the Al-Qaeda core to underscore its narrative of a Western war against Islam. Using its role as the vanguard of the Salafi-jihadi movement, it aims to promote a "clash of civilizations" between the West and Islam. The allure of Al-Qaeda's ideology and narrative draws adherents across the globe. It manifests itself in legitimate terrorist threats, whether through known global affiliated groups or in the actions of individuals who have been radicalized via the Internet.

AFFILIATED GROUPS LINKED TO AL-QAEDA

Al-Qaeda has also leveraged affiliated groups across the globe to attack the U.S. homeland. Prior to his assassination, former Al-Qaeda leader Osama bin Laden successfully impelled Salafi-jihadi groups worldwide to fight against the "near enemy"—their own governments—as well as the distant or "far enemy," the West, specifically the United States. These local groups are becoming more globalized and centralized in their aspirations and objectives as a result of this allegiance.

Affiliated groups constitute an important component of the Al-Qaeda network. Some groups, such as Al-

Jihadi plots in preparation in the U.S. from 2002–2010.
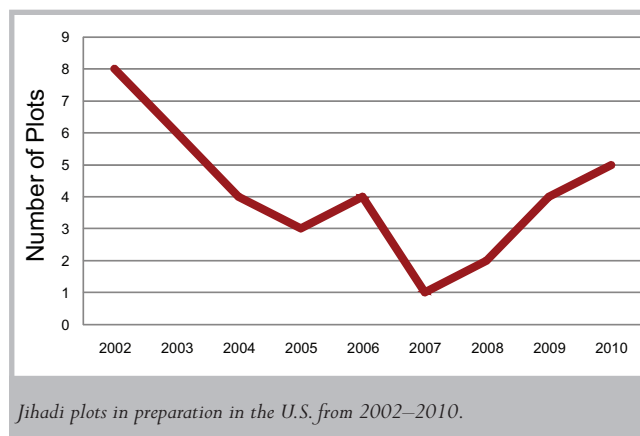
Qaeda in the Islamic Maghreb (AQIM) and Al-Qaeda in the Arabian Peninsula (AQAP), have publicly claimed allegiance to Al-Qaeda. Others, such as the Tehrik-i-Taliban Pakistan (TTP), Lashkar-e-Taiba (LeT), and Harkat-ul-Jihad e-Islami (HUJI), have adopted Al-Qaeda's jihadist ideology and cooperate with the core group, but do not directly claim allegiance in order to maintain their own independence.

Currently, the most active affiliated group is Al-Qaeda in the Arabian Peninsula (AQAP). The AQAP formed in January 2009 when the branches of Al-Qaeda operating in Yemen and Saudi Arabia joined under the leadership of Nasser Abdel Karim al-Wahishi, a Yemeni national with close ties to Al-Qaeda senior leadership. This militant group has expanded its terrorist plots beyond Saudi Arabia and Yemen, as demonstrated in 2009 by the group's failed attempt to explode a bomb on a flight over Detroit on Christmas Day. Several other recent incidents in the U.S. have also been linked to AQAP. A shooting in June 2010 by Abdulhakim Mujahid Muhammad, a self-professed AQAP operative, outside a military recruiting station in Little Rock, Arkansas, killed one recruiter and wounded another; and Army Major Nidal Hasan, also connected with AQAP, staged a November 2009 massacre at Fort Hood, Texas that claimed the lives of 13 people.

The Somali Islamist insurgent group Al-Shabab is also a grave concern for U.S. security agencies. In September 2009, the group formally pledged allegiance to Al-Qaeda, and has been involved in recruiting Somali-Americans and other American Muslims to fight in the civil war in Somalia. American counterterrorism officials have not discounted the possibility that Al-Shahab could recruit Somali-American citizens to carry out future terrorist attacks in the United States.

Homegrown Jihadi Groups

Since 9/11, jihadi operatives "homegrown" in the U.S. have been on the rise. These "self-starters" are inspired by Al-Qaeda or its affiliates, but may have little or no actual connection to these militant groups. Homegrown jihadis represent the broadest layer of the Al-Qaeda network and tend to be radicalized segments of migrant and diaspora communities. Since 2001, several plots in the U.S. have been linked to individuals from various states including Illinois, New Jersey, New York, North Carolina, and Texas.

The homegrown network conforms to the model of decentralized terrorism-inspired groups. The concept is defined by key Al-Qaeda strategist Mustafa Al-Suri's doctrine of *nizam la tanzim* (system, not organization). In his view, the future of jihad consists of small autonomous groups having decentralized organizational structures with no official links to Al-Qaeda leadership; thus, even if the senior hierarchy is dismantled, the threat from Al-Qaeda will persist.

Homegrown plots undermine the previously widespread assumption that American Muslims, unlike their European counterparts, are immune to radicalization. Many counterterrorism experts have argued that the homegrown jihadi terrorism threat in Europe is due to the lack of integration among the immigrant Muslim population and that radicalization is the subsequent by-product of the failed integration. In contrast, Muslim immigrants in the U.S. have more successfully integrated, making them immune to radicalization. The wave of homegrown U.S. jihadist arrests seems to demonstrate, however, that radicalization has indeed affected a small minority of American Muslims.

Due to the highly decentralized structure of the homegrown groups, they are very difficult to identify and apprehend. This problem is compounded if the homegrown operative is a "lone wolf" who does not seek any type of external help. However, homegrown operatives have tended to show poor operational skill—particularly in regard to attack planning, surveillance, and bomb-making. To date, a majority of the homegrown jihadi plots have been crude attempts by operatives lacking the sophistication and experience needed to mount a successful attack. Homegrown terrorists also commonly do not comprehend the limitations their lack of skills present, leading them to attempt attacks that have very little chance of succeeding without assistance and support.

In order to overcome technical deficiencies and strengthen their competence, homegrown terrorists reportedly have begun to reach out for external assistance, using the Internet to identify and connect with networks throughout the world, hoping to build relationships and gain expertise. Some have traveled overseas to establish contacts with various jihadist outfits to acquire operational skills. In the future, a homegrown cell with the skills and knowledge obtained from Al-Qaeda or a similar terrorist group could potentially reach a sufficiently operational acumen to execute a successful terrorism macro attack.

The U.S. Terrorism Threat Landscape

Currently, the U.S. faces a weakened jihadi threat, but one that is still capable of causing significant acts of terrorism. Al-Qaeda has proven to be a highly resilient U.S. adversary, and the rise of homegrown and affiliated Al-Qaeda groups has changed the U.S. terrorism threat landscape. Although operationally weakened, the

Subway lines and stations are at an increased risk of attack.

Jihadi groups and individuals linked to Al-Qaeda will continue to focus on attacking commercial aviation targets.

determination of Al-Qaeda's leaders to attack the U.S. remains unabated. This intent could strengthen when the group feels threatened or vulnerable, but another attack on the scale or magnitude of 9/11 in the near future is unlikely.

The U.S. will continue to experience Al-Qaeda plotting, mostly from individual operatives and affiliated organizations that now target the American homeland. Given the limited technical acumen of these groups and the strengthened U.S. counterterrorism environment, smaller but still deadly plots that circumvent security measures, such as car bombs or armed attacks on urban metropolitan areas are the more likely attack scenarios. Attacks may be similar in scale to the July 2005 London bombing, which killed 52 people.

In terms of target selection, hotels and other economic and business entities are key targets, since many jihadi groups lack the ability to attack more secure "hard" targets such as government buildings, embassies, and military bases, particularly those outside of global conflict zones. Transportation infrastructure, such as subway lines and stations, will also be targeted due to the high density of people, and the disruptive impact of an attack on transportation. And, the public nature of the above locations makes it is difficult to exclude those with hostile intentions.

Jihadi groups and individuals linked to Al-Qaeda also will continue to focus on attacking commercial aviation targets. The near-success of the 2009 Christmas Day plot to bring down an airplane over Detroit, as well as the arrest of Rajib Karim in February 2011 who was charged with attempting to blow up an airliner bound for the U.S., clearly indicate that jihadists will continue to attack aviation targets, despite the high levels of security.

Finally, the terrorism threat in the U.S. will remain primarily an urban phenomenon. For the Muslims around the globe that Al-Qaeda is trying to influence and recruit, an attack on an obscure city or town in America would have little to no impact. Therefore, Al-Qaeda's focus will stay on more populated or well-known cities. Of the nearly 40 jihadi plots in the U.S. since 2001, more than 90% have been attempted in major metropolitan areas. ■

Notes and References

1. Anonymous, "Imperial Hubris: Why the West Is Losing the War on Terror," Brassey's Inc, 2004, Pg. 212.

2. Byman, Daniel, "Scoring the War On Terrorism," National Interest, Summer, 2002, Pg 77.

3. Carrie, Johnson & Hsu, Spencer, "Najibullah Zazi pleads guilty in New York subway bomb plot," Washington Post, February 23, 2010.

4. Anonymous, "Imperial Hubris: Why the West Is Losing the War on Terror," Brassey's Inc, 2004, Pg. 212.

5. Habeck, Mary, "Knowing The Enemy: Jihadist Ideology and the War On Terror," Yale University Press, Pg. 85.

6. Brooke, Steven, "Strategic Fissures: The Near and Far Enemy Debate," Assaf Moghadam and Brian Fishman (eds) Self Inflicted Wound , Debates and Divisions within Al-Qaeda and its periphery," Combating Terrorism Center at West Point, December 10, 2006, Pg. 53.

7. Department of Justice, "U mar Farouk Abdulmutallab Indicted for Attempted Bombing of Flight 253 on Christmas Day," January 6, 2010, http://detroit.fbi.gov/dojpressrel/pressrel10/de010610.htm, (accessed on June 2, 2011).

8. Sudarsan, Raghavan, "American Cleric says he was confidant to Hasan," Washington Post, November 16, 2009 and James Dao, "Man Claims Terror Ties in Little Rock Shooting," The New York Times, January 22, 2010.

9. "Somali militia pledges fealty to bin Laden," Washington Times, http://www.washingtontimes.com/news/2009/sep/23/somali-militia-pledges-allegiance-to-bin-laden/September 23, 2009 (accessed on June 2, 2011).

10. Brynjar, Lia, Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus'ab Al-Suri, Hurst & Columbia University Press, Pg. 121, 2008.

11. Bergen, Peter & Hoffman, Bruce, "Assessing the Terrorist Threat: A Report of the Bipartisan Policy Center's National Security Preparedness Group" Bipartisan Policy Center, September 10, 2010, Pg. 12.

12. Gilles, Kepel, The War for Muslim Minds: Islam and the West, Belknap Press of Harvard University Press, September 21, 2004, Pg. 25.

13. Bergen Peter, & Hoffman, Bruce, "Assessing the Terrorist Threat: A Report of the Bipartisan Policy Center's National Security Preparedness Group" Bipartisan Policy Center, September 10, 2010, Pg. 15.

14. Bjelopera, Jerome, "American Jihadist Terrorism: Combating a Complex Threat" Congressional Research Service, December 7, 2010, Pg. 10.

15. Stewart, Scott & Burton, Fred, "Paying Attention to the Grassroots", Stratfor, August 5, 2009.

16. Sullivan, Kevin, "Four Guilty In London Transit Bomb Plot", Washington Post, July 10, 2007.

17. Vinograd, Cassandra "BA worker jailed for 30 years for plane bomb plot," Washington Post, March 18, 2011.

4 THE POST-9/11 U.S. COUNTERTERRORISM LANDSCAPE

Understanding the counterterrorism environment is as fundamental to the assessment and management of terrorism risk as understanding the threat landscape itself. Since the 9/11 attacks, the U.S. has undertaken significant efforts to improve its defense against terrorist attacks, instituting new security organizations, policies, and procedures; improving intelligence sharing; and increasing the allocation of resources dedicated to counterterrorism. This chapter reviews the changes to the U.S. counterterrorism landscape since 9/11, and concludes with RMS' view of the future U.S. counterterrorism landscape.

COUNTERTERRORISM'S ROLE IN MITIGATING TERRORISM RISK

Natural catastrophes such as earthquakes and hurricanes tend to inflict the greatest damage on the weakest structures, in keeping with the laws of physics. This damage can be mitigated by reinforcing the structures to reduce their vulnerability to the hazard. The ability to alleviate the hazard itself, however, is beyond human control. In contrast, terrorism is a man-made hazard, and thus both the attack frequency and level of damage can be mitigated by the terrorist opposition. Following a major terrorist attack, the level of counterterrorism response intensifies to face the increased threat. Each subsequent event serves to further strengthen this response, helping to reduce attack frequency and improve a nation's ability to control the threat, mitigating terrorism risk.

POST-9/11 U.S. SECURITY IMPROVEMENTS

The 9/11 attacks acted as a catalyst for major changes in U.S. homeland security efforts. The attacks altered not only how the nation would identify and prepare for threats, but how it would work to stop them. The post-9/11 attack responses that have served to mitigate the terrorist threat most significantly include the following.
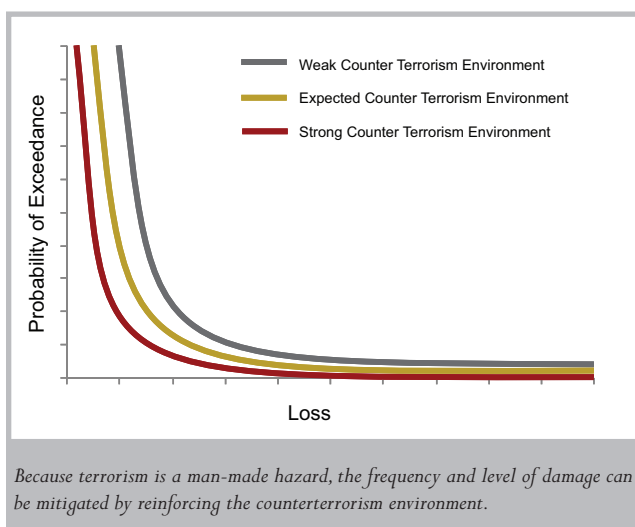
Establishment of Domestic Security Institutions

Since 9/11, the U.S. has established a number of domestic security institutions, including the Homeland Security Council (HSC), the Department of Homeland Security (DHS), the Transportation Security Administration (TSA), and the National Counterterrorism Center (NCTC). These institutions have been instrumental in helping strengthen U.S. security—most notably DHS' efforts to assimilate the counterterrorism activities of the federal, state, and local governments into one cohesive unit. To date, more than 180,000 personnel from over 20 different organizations have become part of the Department of Homeland Security, completing the largest government reorganization since the start of the Cold War, and representing one of the most significant achievements in post-9/11 homeland security.[1]

Nearly a decade later, despite its push for further integration, the DHS continues to search for organizational coherence and assimilation of its core management functions. Nevertheless, most homeland security analysts believe that the DHS has been successful in constraining the ability of groups such as Al-Qaeda to attack the U.S. homeland, and has also led terrorist groups to perceive the U.S. as a more difficult target to strike.[2]

Counterterrorism Legislation

Post-9/11 counterterrorism legislation such as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001"—commonly known as the USA PATRIOT Act or Patriot Act—has been instrumental in pursuing suspected terrorists and dismantling terrorism plots before the public is aware of any potential danger. While much discussion surrounding the Patriot Act has focused on the questioning of civil liberties, particularly over concerns about losing the right of due process and unknowingly putting individuals under surveillance, proponents of the Act have claimed that no part of it has been found unconstitutional, and in most cases its provisions have similar safeguards as standard criminal investigative tools.

The Patriot Act details a number of law enforcement tools and methods intended to help domestic security agencies share and disseminate information, and to more effectively stop the flow of information and resources

Because terrorism is a man-made hazard, the frequency and level of damage can be mitigated by reinforcing the counterterrorism environment.

Emergency response practice drills coordinated by the Department of Homeland Security include this response to a simulated biochemical terrorist attack in New York.

between terrorist groups. Provisions of the Patriot Act, such as the routine use of roving wiretaps, have assisted counterterrorism agencies in conducting continuous surveillance of terrorist suspects across different modes of communication. U.S. counterterrorism practitioners used roving wiretaps to prevent several macro terrorism attacks, including thwarting Najibullah Zazi's September 2009 plot to bomb the New York subway system.[3] Thus, while a fair amount of disagreement surrounds the Patriot Act, successes such as the arrest of Najibullah Zazi illustrate its continued importance to counterterrorism efforts.

Enhancements to Counterterrorism Intelligence Capabilities

Since the 9/11 attacks, U.S. domestic intelligence and security organizations have made an extensive effort to improve counterterrorism intelligence by streamlining communication among the different levels of U.S. law enforcement, which prior to the attacks were highly decentralized—in addition to federal and state policing, U.S. systems extend to county and municipal agencies, among others. This decentralization is an asset because it keeps U.S. law enforcement agencies attuned to their local surroundings and directly accountable to their communities. But it is also a liability, particularly in the post-9/11 environment, as information sharing plays a fundamental role in thwarting terrorism plots and the sheer number of agencies often hinders communication.

To improve law enforcement's intelligence-sharing capabilities, the U.S. has established "fusion" centers to pool information from all levels of law enforcement across the country. The centers' primary responsibility is to ensure that different levels law enforcement agencies are apprised of current and emerging trends that threaten the security of relevant areas or jurisdictions. As of 2011, 72 centers are in operation across the country.[5] The centers have expanded their role, and now have the mandate to support counterterrorism operations in

addition to analyzing and disseminating information on terrorist threats.

Improvements to Border Security

With over 90 million foreign visitors passing through U.S. international airports annually, and more than 16,000 large shipping containers arriving at U.S. ports every day, the control of people and goods crossing U.S. borders is a constant challenge.[6] Nevertheless, since 9/11, much progress has been made toward strengthening border security. To extend its reach, U.S. security forces have pushed the border outward to allow inspections of travelers and goods in overseas ports. To strengthen the border inspection process, high-end technology, such as biometric identifiers in travel documents and shipment containers for the shipment of goods, has been implemented.[7] And, the process of "profiling out" less threatening people and goods helps security officials focus on targets that require more attention. These policies have made border control much more manageable, but given the complexity of the environment and the high volume of activity along U.S. borders, cannot guarantee complete security.

THE FUTURE U.S. COUNTERTERRORISM LANDSCAPE

Much of the homeland security framework implemented in the wake of 9/11 will continue for the foreseeable future. There have been dramatic increases in spending on security and an expansion of capacity to prevent and respond to terrorist attacks at all levels of government. But, given the austere fiscal environment of today, and the lack of any successful major terrorism plots on U.S. soil since 9/11, legitimate concerns about the appropriate level of spending for homeland security have been raised, and further large-scale investments appear unlikely. Moreover, the past decade has made it increasingly apparent that securing the homeland is an expensive endeavor. Thus, we will likely see a greater push toward better allocation of resources instead of large increases in spending on homeland security—considerations such as the amount of spending for airline security compared with maritime and rail security will become the types of issues addressed in the future.[8]

Related to the importance of resource allocation is the role of technology in protecting the U.S. homeland. Technological approaches have played a crucial role in reducing the threat of terrorist attack. The U.S. border patrol currently leverages unmanned aerial vehicles (UAV) in border controls, and the role of technology in the homeland security arena will continue to grow. Future technological innovation will help to enhance

counterterrorism effectiveness, reduce its cost, and lessen the burden of security measures on the public they are meant to protect.

Lastly, terrorism is a derivative of extremism. Thus, unless extremism is controlled, the threat of terrorism will persist. The current focus of U.S. law enforcement is to disrupt terrorist operations. This reduces the immediate threat of a terrorist attack by limiting the operational space of such groups. However, the U.S. has not attempted to counter the radical ideology with which such groups are imbued. This is a major strategic oversight, as a surviving ideology helps to resuscitate a weakening terrorist group by inspiring a stream of willing recruits to replace those who were captured or eliminated.[9]

The Department of Homeland Security would benefit from developing initiatives aimed at preventing the future radicalization of vulnerable communities. By investing in community engagement programs to reduce the appeal of such movements, the DHS could work to counter Muslim misconceptions about the U.S. and promote community goodwill.[10] Such initiatives help to reduce the appeal of radical ideology and make it more difficult for extremists to penetrate the Muslim community—particularly relevant in light of the increase of the homegrown jihadi threat in America. They could also reduce the probability of recruitment, fundraising, procurement, and other support and operational functions.

Remaining Vigilant

Since 9/11, U.S. federal, state, and local governments have joined forces to help protect the country from terrorism. As a result, from symbolic landmarks, to public celebrations, to border crossings and critical infrastructure, U.S. homeland security defenses are better and stronger today than they were a decade ago.

While the absence of further macro scale attacks indicates that the U.S. is better protected from the threat of terrorism, improved security may not always translate to improved safety. Al-Qaeda and its affiliated groups' intentions to attack the U.S. remain strong. The spread of radical Islamic ideology has yet to diminish. Thus, even with effective security measures in place, the Department of Homeland Security and related U.S. agencies must remain vigilant and focused on strengthening security-related policies as we move into the future. ■

Notes and References

1. Heyman, David, & Ridge, Eric, "American Domestic Security," Julianne Smith & Thomas Sanderson (eds), "Five Years After 9/11: An Assessment of America's War on Terror" Center for Strategic and International Studies, 2006, Pg. 15.

2. For additional information on U.S. Homeland Security, see Seth Jones "Terrorism and the Battle for Homeland Security," in Russell D. Howard, James J.F. Forest and Joanne Moore (eds.), Homeland Security and Terrorism, 2005; Michael Kraft, "The U.S. Government's Counterterrorism Research and Development Programs," in James J.F. Forest (eds.), Countering Terrorism in the 21st Century, Vol. 1: Strategic and Tactical Considerations, 2007; and Clark Ervin, Open Target: Where America is Vulnerable to Attack. Palgrave Macmillan, May 2006.

3. Kornblut, Anne, "Obama Team Says Zazi Case Illustrates Balanced Approach to Terror Threat," Washington Post, October 6, 2009.

4. Report from the 2011 National Fusion Center Conference, March 24, 2011, http://www.ise.gov/news/report-2011-national-fusion-center-conference, (accessed on June 2, 2011).

5. Rollins, John & Connors, Timothy, State Fusion Center Processes and Procedures: Best Practices and Recommendations, Policing Terrorism Report, September 2007, http://www.manhattan-institute.org/html/ptr_02.htm, (accessed on June 2, 2011).

6. Riley, Jack, Border Controls, RAND Infrastructure, Security & Environment, 2006, http://www.rand.org/pubs/reprints/2006/RAND_RP1216.pdf, (accessed on June 2, 2011).

7. Ibid.

8. Rees, William S. Jr. & Gates, Kevin, "DHS Science and Technology Initiatives in Critical Infrastructure Protection," in James J.F. Forest (eds.), Homeland Security: Protecting America's Targets, Vol. 3: Critical Infrastructure, Westport, 2006.

9. de Wijk, Rob, "The limits of military power" in Alexander T. Lennon (eds.), The battle for hearts and minds: using soft power to undermine terrorist networks. MIT Press, 2003.

10. Gunaratna, Rohan, "The Global Jihad Movement: The Context of the Threat" Homeland Security 2015: The Proceedings of a Workshop Convened to Consider Homeland Security in the Year 2015, January 2008, http://ceps.edu.au/userfiles/file/Homeland%20Security%202015%20Workshop%20Proceedings.pdf, (accessed on June 2, 2011).

5 EVALUATING AL-QAEDA'S POST–9/11 CBRN CAPABILITY

The low frequency and high severity of a mass casualty chemical, biological, radiological, or nuclear (CBRN) attack makes the evaluation of such attacks a critical element in the assessment of terrorism risk. Since 9/11, Western intelligence has shown grave concern over Al-Qaeda's intent to use CBRN weapons. Al-Qaeda and its affiliates have been linked to a number of plots attempting to develop or acquire CBRN weapons. However, does Al-Qaeda's CBRN intent match its capability? So far, the answer appears to be no. This chapter reviews Al-Qaeda's CBRN development efforts in the last decade, and discusses why it is unlikely at present that Al-Qaeda will be able to launch such an attack.
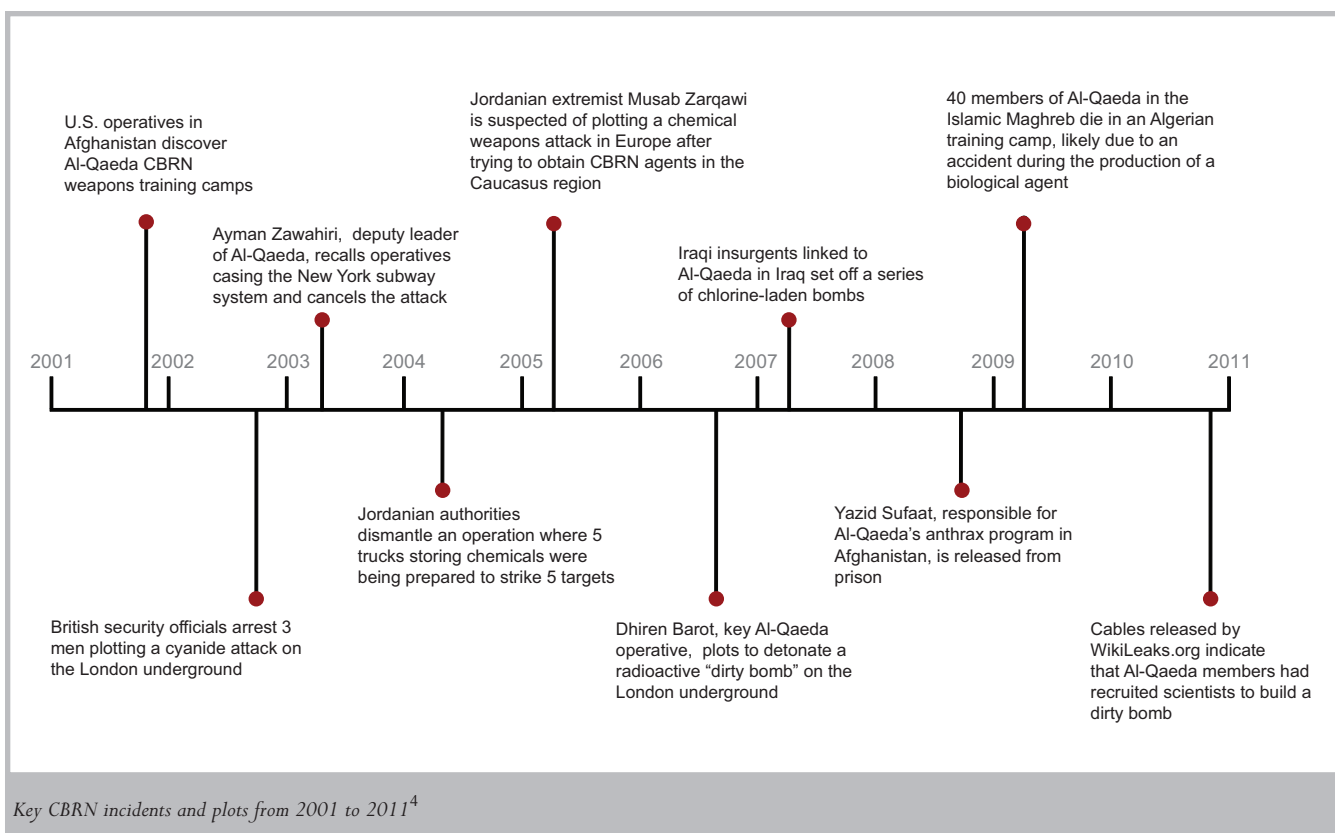
AL-QAEDA AND THE USE OF CBRN AGENTS

Chemical, biological, radiological, and nuclear (CBRN) agents appeal more to religious terrorist groups such as Al-Qaeda than to other types of terrorist organizations.[1] The logic behind this is that while more "secular" terrorist groups might hesitate to kill a large number of civilians for fear of alienating their support network, religious terrorist organizations regard such violence as not only morally justified but expedient for the attainment of their goals.

Al-Qaeda and its affiliates' intent to use CBRN attack modes can be traced back as early as 1999, when Al-Qaeda established its CBRN development program, code-naming it the "Yogurt Project" under the stewardship of Egyptian chemist Abu Khabab Masri.[2] Al-Qaeda followed up its CBRN development by requesting and receiving a fatwa from the Saudi Sheikh Nasir Hamid al-Fahd in 2003 that condoned the use of CBRN agents.[3] Following U.S. "Operation Enduring Freedom" in Afghanistan, most of the infrastructure for CBRN development was destroyed. Nevertheless, there have been numerous reports that Al-Qaeda and its affiliated groups continue to attempt to acquire, weaponize, and use CBRN agents for a terrorist attack.

Equally troubling has been the plethora of information on CBRN agents posted on jihadi websites, message boards, and blogs. Since the 9/11 attacks, Al-Qaeda and its affiliates have released publications, manuals, and statements that discuss the importance and use of various chemical and biological agents as well as the use of nuclear weapons.[5] These online sources contain extensive information on the potency and effectiveness of such agents.

Timeline events (2001–2011):

- U.S. operatives in Afghanistan discover Al-Qaeda CBRN weapons training camps
- Ayman Zawahiri, deputy leader of Al-Qaeda, recalls operatives casing the New York subway system and cancels the attack
- Jordanian extremist Musab Zarqawi is suspected of plotting a chemical weapons attack in Europe after trying to obtain CBRN agents in the Caucasus region
- Iraqi insurgents linked to Al-Qaeda in Iraq set off a series of chlorine-laden bombs
- 40 members of Al-Qaeda in the Islamic Maghreb die in an Algerian training camp, likely due to an accident during the production of a biological agent
- British security officials arrest 3 men plotting a cyanide attack on the London underground
- Jordanian authorities dismantle an operation where 5 trucks storing chemicals were being prepared to strike 5 targets
- Dhiren Barot, key Al-Qaeda operative, plots to detonate a radioactive "dirty bomb" on the London underground
- Yazid Sufaat, responsible for Al-Qaeda's anthrax program in Afghanistan, is released from prison
- Cables released by WikiLeaks.org indicate that Al-Qaeda members had recruited scientists to build a dirty bomb

Key CBRN incidents and plots from 2001 to 2011[4]

The Intent: CBRN Development and Acquisition

Chemical Agents

Experimentation in crude chemical agents was prevalent in Al-Qaeda's camps in Afghanistan prior to 9/11. Today, however, it appears that their use has largely been left to the discretion of individual cells plotting smaller-scale attacks outside the direct control of the Al-Qaeda core leadership. Examples include a Bahraini terrorist cell's plot to use a crude cyanide gas device called the "mobtaker" (an Arabic word roughly meaning "invention") in an attack on the New York City subway system in early 2003; and a late 2005 plot by the Abu Musab al Zarqawi network to use cyanide in multiple attacks in Europe.[6] In cases where chemical plots have been linked to Al-Qaeda jihadist groups, hydrogen cyanide and industrial toxic chemicals such as chlorine compounds appear to be the weapon of choice.[7]

A direct attack on an industrial chemical facility or an assault of a rail car full of toxic chemicals as a means to cause a toxic vapor release is also a possibility. Although not a terrorist attack, the Union Carbide accident that caused a leak of methyl isocyanate gas and other toxic chemicals in Bhopal, India in 1984 illustrated the catastrophic scale of damage that is possible from a chemical release.[8] More than 3,800 fatalities resulted from the accident's initial chemical release, and estimates indicate that more than 200,000 people have been medically affected in the years since.[9]

Biological Agents

Since 2001, several reports have intimated at Al-Qaeda's attempts to procure and weaponize biological agents. For example, in March 2005, French Interior Minister Dominique de Villepin claimed at a world conference on bioterrorism that Al-Qaeda was trying to produce biological agents such as anthrax, ricin, and botulism toxins in the Pankisi Gorge, a rebel-controlled area of Georgia.[10]

Western security services have also expressed public concerns after detecting growing signs of Al-Qaeda's recruitment of scientists in biotech fields. In some cases, Al-Qaeda-linked groups have targeted students, offering to fund academic courses in exchange for using their newly acquired expertise. Reports suggest that these scientists are being groomed for a jihadist biotech research project, which, if true, suggests that Al-Qaeda is taking a long-term view toward building a capability in non-conventional weapons.[11]

Radiological Weapons

A radiological "dirty bomb" is designed to spread fissile radioactive material over an extensive area by combining radioactive material with a conventional explosive. Among the CBRN weapons that a terrorist could launch, the dirty bomb is the most plausible for several reasons. First, radiological materials are readily available, and relatively easy to obtain. Second, terrorists could easily transport the weapon. Third, the skills required to manufacture such a bomb are minor compared to other unconventional weapons.

There have been several reported cases of Al-Qaeda attempting to procure radiological materials. The most famous attempt concerns Al-Qaeda operative Dhiren Barot, who was arrested in the United Kingdom in 2004 for carrying plans to conduct a radiological dispersal device (RDD) attack.[12] Chechen rebels with close links to Al-Qaeda have also demonstrated their capabilities in this area on a number of occasions. In March 1995, Chechen rebels planted but failed to detonate a dirty bomb consisting of dynamite and Cesium 137 in Moscow's Izmailovsky Park.[13]

Nuclear Weapons

Al-Qaeda has consistently shown strong interest in acquiring nuclear weapons and has even called the acquisition of such weapons a religious duty. Its intent is that the devastation of a nuclear attack, coupled with the stark imagery of a mushroom cloud rising over a U.S. city, would alter the course of history, just as the 9/11 attacks have done.

In November 2004, Pakistani journalist Hamid Mir interviewed Al-Qaeda's senior leader Ayman Zawahiri, who told Mir the following:

"Mr. Mir, if you have $30 million dollars, go to the black market in central Asia, contact any disgruntled Soviet scientist and a lot of dozens of smart briefcase bombs are available. They have contacted us, we sent our people to Moscow to Tashkent to other central Asian states and they negotiated and we purchased some suitcase bombs."[14]

Several press reports have also circulated regarding Al-Qaeda and other jihadi groups inquiring about nuclear weapons. For example, in 2005, German authorities arrested Al-Qaeda member Ibrahim Muhammad for attempting to buy uranium isotopes on the combat arms black market in Luxembourg. Documents seized in Afghan training camps in late 2001 also indicate a rudimentary understanding of nuclear fission devices. There have also been unverified reports of nuclear weapons acquisition from countries of the former Soviet Union.

Despite the obstacles and technical challenges, Al-Qaeda's interest in a CBRN arsenal has yet to diminish due to the potential for high-severity outcomes that conventional attacks cannot produce.

Not limited to attempts at nuclear fission materials acquisition, Al-Qaeda and its affiliates have also attempted to attack nuclear power installations targets. Nuclear power plants in Australia, Canada, and France have all been targeted in the last ten years by groups or individuals linked to or inspired by Al-Qaeda.

The Capability: Technological and Logistical Hurdles

Since Al-Qaeda lost its sanctuary in Afghanistan in late 2001, the group has evolved into a much more decentralized organization relying on autonomous cells or affiliated groups to carry out its attacks. While this makes the organization harder to detect and counteract, lack of centralized control also prevents Al-Qaeda and its affiliates from pooling their resources to develop a true mass-casualty CBRN capability. Continued pressure from counterterrorism forces compounds the groups' inability to establish an operational environment suitable for a sustainable CBRN development program.

In general, the technological hurdles involved in perpetrating a mass CBRN incident remain significant and should not be discounted. Although CBRN attack threats receive widespread publicity, in reality, few large-scale terrorist attacks using CBRN agents have been successful. The most notable exception occurred in 1995, when the Japanese cult, Aum Shinri Kyo, successfully inflicted a major chemical attack on the Japanese populace. The cult released sarin gas into the Tokyo subway system, killing 19 individuals and injuring more than 5,000.[15] The success of Aum Shinri Kyo

was a result of their operational capabilities: the cult was believed to have $1 billion in assets at its disposal, a dozen biologists working in research facilities, and the access as well as the autonomy to experiment and develop a range of chemical and biological agents.[16] In sharp contrast, Al-Qaeda's current operational state is that of an organization on the run, with limited resources, and lacking both technical expertise and its inspirational leader, Osama bin Laden. Thus, Al-Qaeda's current ability to orchestrate a successful CBRN attack seems compromised at best.

Moreover, an examination of the information on CBRN agents disseminated by Al-Qaeda and fellow jihadist groups via cyberspace does not instill much confidence regarding the groups' technical acumen to execute such an attack. While most of the technical data on jihadi websites and message boards is valid and accurate, the literature does not offer specific instructions on other important factors, including weaponization, manufacture of agents, and effective deployment[17]— crucial considerations for successful orchestration of a CBRN attack.

Concerns over a nation state covertly providing a CBRN weaponized agent to a terrorist group appear exaggerated as well.[18] National governments are unlikely to provide such materials to terrorist organizations like Al-Qaeda as they have no control over such groups. In addition, giving a terrorist group a CBRN agent would expose the donor state to a massive retaliation once the attack had been executed. Just as states will not provide CBRN agents to any terrorist organization, they are highly unlikely to sell them either. This leaves the alternative of stealing CBRN agents from a nation state; but as most states are very meticulous about the security measures implemented around such weapons, a successful theft would be unlikely.[19]

Current and Future CBRN Threat

Al-Qaeda has long plotted to acquire and launch CBRN weapons. In addition to the statements the group has made about its desire to obtain and use such weapons, there is enough credible information in the last decade to show that Al-Qaeda has at least a nascent CBRN program. Fortunately, obtaining a CBRN capability capable of killing hundreds, much less thousands, is a technical challenge they have yet to overcome.

Current evidence suggests that Al-Qaeda and its affiliates are still far from such capabilities, and at best can only produce crude CBRN agents that are more suited for smaller attacks. As a result, the groups will continue to leverage conventional attack tactics such as car or truck bombs and perhaps armed suicide

attacks rather than attempting the riskier and potentially more expensive execution of a massive CBRN attack. Nevertheless, this does not preclude Al-Qaeda or its affiliates from deploying a CBRN weapon in the future. Despite the obstacles and technical challenges, Al-Qaeda's interest in a CBRN arsenal has yet to diminish due to the potential for high severity outcomes that conventional attacks cannot produce. Thus, Al-Qaeda is likely to remain relentless in its pursuit to overcome its capability constraints, making this a case not of "if," but rather "when," an Al-Qaeda CBRN attack will occur. ∎

Notes and References

1. For additional information on CBRN agents and religious terrorist groups, see Gavin Cameron's "WMD Terrorism In the United States, The threat and possible counter measures," Non Proliferation Review, Spring 2000; Bruce Hoffman's "Change and Continuity in Terrorism," Studies in Conflict and Terrorism, vol. 24, No. 5, September 2001; Jean-François Mayer's, "Cults, Violence, and Religious Terrorism: An International Perspective," Studies in Conflict and Terrorism, vol. 24, no. 5, September 2001; and John Parachini's, "Putting WMD Terrorism into Perspective," The Washington Quarterly, vol. 26, no. 4, Autumn 2003.

2. Darling, Dan, "Al-Qaeda's Mad Scientist" The Weekly Standard, January 19, 2006.

3. Sheikh Nasir bin Hamid al-Fahd, "A Treatise on the Legal Status of Using Weapons of Mass Destruction Against Infidels," Open Source Center, Arabic Text in Arabic, May 2003.

4. Data from RMS Terrorism Incident Catalog.

5. For more information see Sammy Salama and Lydia Hansell's "Does Intent Equal Capability? Al-Qaeda and Weapons of Mass Destruction," Nonproliferation Review, Vol. 12, No. 3, http://cns.miis.edu/pubs/npr/vol12/123/123salama.pdf (accessed on June 2, 2011).

6. Scheuer, Michael, "New York Subway Plot and al-Qaeda's WMD Strategy, Terrorism Focus," Terrorism Focus, Volume: 3 Issue: 24 http://www.jamestown.org/programs/gta/single/?tx_ttnews[tt_news]=814&tx_ttnews[backPid]=239&no_cache=1 (accessed on June 2, 2011).

7. Pita, René, "Assessing al-Qaeda's Chemical Threat," International Journal of Intelligence and Counter Intelligence, Volume 20, Issue 3, September 2007, Pg. 480.

8. Broughton, Edward, "The Bhopal disaster and its aftermath: a review," Environ Health, May 10, 2005, Pg. 4.

9. Ibid.

10. MacVicar, Sheila & Schuster, Henry, "European terror suspects got Al-Qaeda training, sources say," CNN, http://articles.cnn.com/2003-02-06/us/sprj.irq.alqaeda.links_1_zarqawi-chemical-weapons-abu-khabab?_s=PM:US (accessed on June 2, 2011).

11. Townsend, Mark, "Terrorists try to infiltrate UK's top labs," The Guardian, November 2, 2008.

12. Hoffman, Bruce, "CBRN, Terrorism Post 9-11," in Howard, Russell D. and Forest, James J.F. (eds.) Terrorism and Weapons of Mass Destruction McGraw-Hill, March 2007.

13. Allison, Graham & Kokoshin, Andrew, "The New Containment: An Alliance Against Nuclear Terrorism," in Juliette N. Kayyem and Robyn L. Pangi (eds.), First to arrive: state and local responses to terrorism, September 2003, Pg. 12.

14. Badkhen, Anna, "Al-Qaeda Bluffing About Having Suitcase Nukes, Experts Say," San Francisco Chronicle, March 23, 2004.

15. Cameron, Gavin, "Multi-track Microproliferation: Lessons from Aum Shinrikyo and Al-Qaeda," Studies in Conflict and Terrorism, vol. 22, no. 4 (Nov 1999), Pg. 278.

16. Ibid.

17. Salama, Sammy & Hansell, Lydia, "Does Intent Equal Capability? Al-Qaeda and Weapons of Mass Destruction," Nonproliferation Review, Vol. 12, No. 3, http://cns.miis.edu/pubs/npr/vol12/123/123salama.pdf (accessed on June 2, 2011).

18. Bergen, Peter, "Reevaluating Al-Qaida's Weapons of Mass Destruction Capabilities," Combating Terrorism Center (CTC) Sentinel, September Issue, http://www.ctc.usma.edu/posts/reevaluating-al-qaida%E2%80%99s-weapons-of-mass-destruction-capabilities, September 1, 2010.

19. Ibid.

A Dirty Bomb Scenario

The prospect of a terrorist attack using a radiological dispersal device—a dirty bomb—is among the most serious and plausible of all chemical, biological, radiological, or nuclear (CBRN) terrorist threats.

Building the Bomb

Obtaining material to prepare a dirty bomb that releases significant amounts of radioactivity is not a trivial undertaking, since likely sources of bomb material are stringently monitored in the U.S. and other Western countries. Sources of radioactive material include spent nuclear fuel rods, as well as medical and commercial devices used for irradiation and measurement, which contain radioactive isotopes such as Cesium-137 and Cobalt-60.

Once radiological material is collected, it is milled into a powder; finer particles disperse over a greater area and penetrate deeper into the respiratory system, leading to a more lethal uptake. The preparation process requires industrial equipment that can produce powders on the order of 1 micron in diameter, as well as significant technical sophistication, not the least in ensuring that the preparers of the bomb are not exposed to the finely ground material.

The Attack

To inflict maximum damage, radioactive material is most likely to be dispersed using a small explosive in the commercial business district of a major city, as plots involving aircraft are much more likely to be interdicted. The area impacted by a dirty bomb attack would be much smaller than that from a true nuclear bomb explosion or an attack on a nuclear power plant. And, the relatively low dispersal of radioactivity would imply that fewer people would be exposed to a level of radioactivity that would pose a significant acute or long-term health risk. Implementation of a timely and appropriate response would minimize exposure to the population at large.

Post-Event Impacts

The principal impact of a dirty bomb attack would be the forced evacuation and decontamination of a large area to meet the criteria for protection of public health. Dirty bombs can cause prolonged business closures while the extent of contamination is determined and a decontamination strategy is decided upon. As a result, business interruption losses are expected to be disproportionately high relative to the

Hazard footprint from a dirty bomb attack in downtown Manhattan.
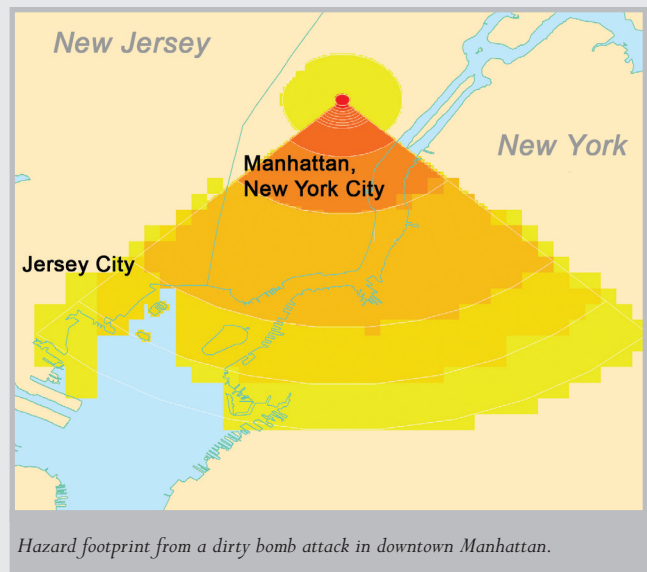
actual contamination level for a property.

The U.S. Department of Homeland Security has issued Protective Action Guidelines that prescribe (but do not mandate) response actions in the aftermath of a dirty bomb explosion. The guidelines divide the response into three broadly defined and overlapping phases. The first phase occurs immediately after the event, and involves taking the appropriate measures for minimizing population health risk. The DHS recommends a combination of sheltering in place and orderly evacuation. In the intermediate term, the responders and local regulatory agencies are given a general framework for determining how to characterize the extent of impact and devise long-term solutions for restoration. In the final, long-term phase, remediation projects are initiated with the goal of restoring as much of the area as possible.

Significantly, the guidelines stop short of prescribing long-term remediation levels, in order to balance the need to expeditiously restore access to economically vital areas with the need to ensure maximum public health protection. However, this decision has led to concerns that any ad hoc cleanup criteria set up in the shadow of such an event would not be as protective as other remediation criteria mandated by the EPA, and would consequently not meet with public acceptance, which is vital to ensuring effective event response. As indicated by the experience of setting of risk-based standards for cleanup of superfund sites, the issue of determining the right amount of cleanup has a major influence on the amount of time and money required for long-term remediation and is likely to be the most contentious part of the long-term response.

6 MODELING TERRORISM FREQUENCY

One of the more contentious components of terrorism risk modeling is the estimation of attack frequency. The ability to realistically model the annual frequency of major terrorist attacks can seem as impossible as the ability to forecast individual human actions. However, RMS views frequency modeling to be a realistic and necessary component of terrorism risk management. By using social network analysis instead of expert opinion to understand the resources and constraints that affect terrorist activity, probabilistic models can quantitatively assess attack frequency. This chapter discusses the concepts underpinning RMS' terrorism frequency methodology.

Understanding Attack Frequency

In order to estimate terrorism attack frequency, it is necessary to determine the number of attacks a terrorist organization could feasibly plan and execute in a given year. Feasibility is determined in large part by logistical factors such as time, money, and resources. Resource and financial constraints present a limited obstacle for terrorist groups, particularly in the execution of conventional attacks. Likewise, it is difficult to argue that organizational, production, or other time-dependent factors have a significant impact on attack feasibility.

The apparent absence of rate-limiting factors could raise legitimate concerns that the number of planned attacks could escalate significantly, without warning. Indeed, the unrelenting terrorist attacks in high-risk areas such as Pakistan appear to bear this out. Thus, given Al-Qaeda's long-stated intent to inflict maximum loss on the West, why are terrorist bombings not a regular occurrence on the streets of Western cities such as London, New York, or Paris, as they are in Lahore? The answer lies not in the actions of individual terrorists or the study of human behavior, but in the analysis of the social networks in which terrorists operate.

Using Social Network Analysis

The principal scientific basis for understanding terrorism attack frequency lies within social network analysis. Social networks are amenable to quantitative probabilistic analysis in a way that individual human behavior is not. Irrespective of the behavior of the terrorists themselves, the frequency of successful attacks is regulated by the universality of human social networks, in the real world as well as online. Regardless of a terrorist's location, thoughts, or actions, his electronic communications can be monitored, and his contacts can be checked. Communications between terrorists

and those in their social networks can be intercepted by the law enforcement, security, and intelligence services to interdict plots before terrorists move toward their targets.

Using quantitative social network analysis to estimate attack frequency reduces the reliance on qualitative expert judgment, marking an important advance in

The principal scientific basis for understanding terrorism attack frequency lies within social network analysis.

probabilistic terrorism modeling in the post-9/11 era. While some dependence on expert judgment is inevitable due to gaps in empirical data, probabilistic modeling aims to minimize subjectivity to the fullest extent possible, to help reduce uncertainty in model results. Guided by this principle, and aided by the wealth of new information available in the decade since 9/11, the RMS probabilistic terrorism model calculates attack frequency with a parsimonious number of quantitative parameters, minimizing the incorporation of subjective expert judgment.

In the asymmetric war with terrorists, the forces of the state have a vast superiority in the domain of communications security. Even on those rare occasions where a terrorist plot is not interdicted, the terrorists' social networks help detectives identify the criminals quickly. For example, the July 2005 suicide bombing on the London Underground was successful; and unlike 9/11, there was no ready list of passengers from which detectives might identify the culprits. But Scotland Yard managed rapidly to infer the names of the suicide bombers through social network leads. First, forensic investigators found evidence linked to suspected terrorist Mohammed Siddique Khan at two of the bomb sites. There was only a slim chance that this could happen fortuitously. Second,

the worried mother of the youngest suicide bomber, Hasib Hussain, phoned the police hotline to report her 18-year-old son missing.[1] She knew the names of his traveling companions, one of whom was Mohammed Siddique Khan. By connecting the dots through social network analysis, law enforcement agencies were able to profile the individuals involved in the attack, and identify Khan as the presumed leader of the attack.
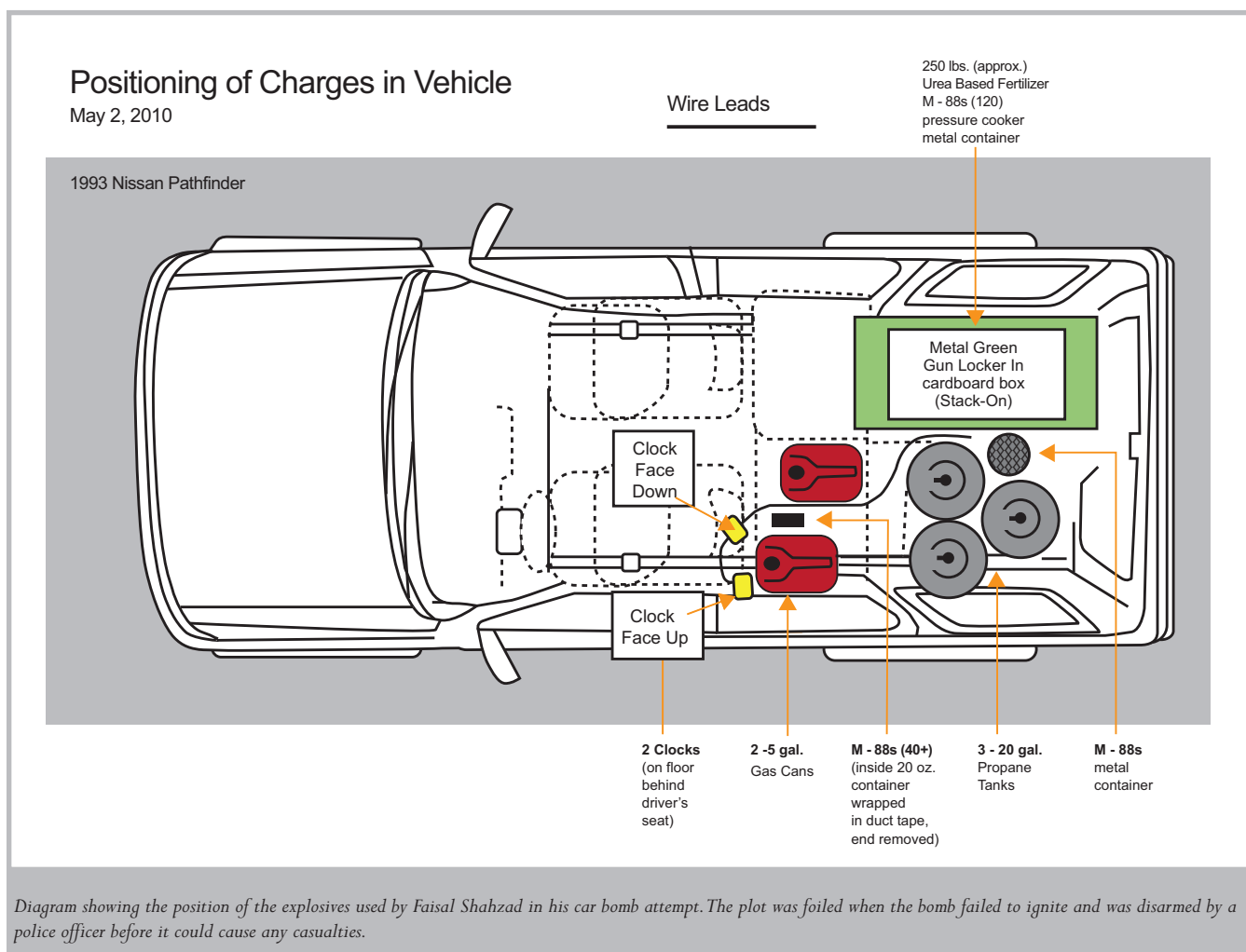
Another noteworthy example of the role of social networks in identifying terrorists was the arrest of Faisal Shahzad, who attempted a car bombing at New York City's Times Square on May 1, 2010.[2] The plot was foiled when the bomb failed to ignite and was disarmed by a police officer before it could cause any casualties. As Shahzad had negotiated the purchase of an SUV using an anonymous disposable cell phone, the FBI was able to retrieve the cell phone number from the SUV seller, and trace the calls made from that cell phone. One call led to a contact name in Pakistan that Faisal Shahzad had given immigration officials when he entered the U.S. a few months earlier, providing the FBI with the connection needed to identify and arrest Shahzad.

The attempted Times Square bombing illustrates a key principle in assessing the relative likelihood of a successful terrorist attack. The success of an attack depends not just on the associated logistical burden of financial, technical, and material resources required, but also on the attack-specific interdiction rates, which are a function of the number of operatives involved in the plot. The more elaborate and ambitious the plot, the more operatives required to carry out the attack. The greater the number of operatives, the greater the likelihood of interdiction. Thus, while large-scale, ambitious plots pose the greatest risk, they are also more likely to be interdicted, decreasing the probability of success. For example, had Shahzad enlisted the help of accomplices, in particular an expert bomb maker, the Times Square plot may have been operationally effective. But, the addition of extra operatives would have made interdiction by law enforcement agencies much more probable.

THE TERRORISM FREQUENCY METHODOLOGY

The success or failure of a macro terror attack plot is determined by the interplay of dynamics between the actions of the terrorists and the counterterrorism actions of the state. The majority of terrorist plots in nations such as the U.S. are interdicted through intelligence and public vigilance (and a touch of good fortune).

Diagram showing the position of the explosives used by Faisal Shahzad in his car bomb attempt. The plot was foiled when the bomb failed to ignite and was disarmed by a police officer before it could cause any casualties.

When a plot is successful, counterterrorism action is commensurate with the threat, and each successful attack is met with a swift counterterrorism response. This response suppresses the threat of future attacks—protecting the public, albeit at a cost of the erosion of some civil liberties through increased surveillance, stricter immigration checks, and harsher interrogation tactics.

The counterterrorism actions following a successful attack influence the likelihood that a subsequent successful attack will occur. In the context of probabilistic modeling, this means that the statistical distribution of successful macro terror attacks is not independent, because countermeasures will be ramped up after any successful attack. Therefore any attacks subsequent to an initial attack cannot be treated as statistically independent, and their probability of occurrence must be modeled using a statistical process that assumes interdependence between the modeling parameters. Thus, terrorism attack frequency is modeled using a "non-Poissonian"[3] process based on the following three input parameters:

- Annual number of planned attacks
- Counterterrorism non-interdiction rate
- Political suppression factor

Annual Number of Planned Attacks

A major factor determining whether a planned attack will succeed or fail is the number of operatives involved in the plot. RMS uses social network analysis to understand how increasing the size of a terrorist cell will increase its chances of detection. This information is used to estimate the constraints on the size and frequency of terrorist attacks. A key observational metric is the number of planned attacks or plots that are discovered in a given city or country. Planned terrorist attacks or plots are categorized as follows:

(a) Plots where alleged terrorists have been arrested and convicted of terrorist offenses

(b) Plots where alleged terrorists have been arrested, but only convicted of non-terrorist offenses, such as immigration violations

(c) Plots where alleged terrorists have been acquitted on all charges

(d) Plots where no arrests have been made

Because this information cannot be compiled until the cases are prepared and heard in court, some lag time is expected. When a case goes to trial, relevant information such as the weapon of attack, the targeting portfolio, and the number of individuals involved in the attack or plot, becomes publicly available and serves as input for the model.

The judicial process provides an evidence-based method for estimating the annual number of terrorist plots. Those in category (a) are included, and those in category (c) are excluded. In some cases, courtroom disclosure may reveal reasonable grounds to believe that a terrorist plot was being planned, even if the admissible evidence was insufficient for a conviction to be obtained. This might happen, for example, if certain incriminating wire-tapping evidence became inadmissible. For modeling purposes, such cases are recognized as real plots belonging to category (a) and not category (b). From time to time, additional information comes to light, via security forces or the media, of a potential plot in the very early stages of development. In general, these cases, classified in category (d), lack the weight of evidence to justify inclusion as genuine plots.

Counterterrorism Interdiction Rate

Where intelligence services are very capable and professional, and there is limited local popular support for terrorism, the great majority of terrorist plots are stopped. Counterterrorism efforts are effective in interdicting attack plots in Western countries, as evidenced by the large proportion of failed plots that have been reported. The RMS terrorism model assumes an interdiction rate range typical of past major terrorist campaigns, in which 80% to 90% of attack attempts are unsuccessful. This assumption is supported by data from Al-Qaeda terrorists themselves. In the confessions of the 9/11 mastermind, Khalid Sheikh Mohammed, released in March 2007, he claimed to have been responsible for 7 successful attacks, but had planned attacks against a further 32 targets that were aborted, a failure rate of 82%, five in every six.[4]

Political Suppression Factor Following an Attack

RMS also considers the upper limit to the number of successful terrorist attacks in a given time period to be controlled by the political response to a severe terrorist attack. In contrast to natural hazard events, which are beyond human control, terrorist attacks in Western countries will elicit a strong government response to mitigate the risk of subsequent attacks. For example, in the U.S., the Patriot Act was drafted rapidly after 9/11. In the U.K., severe legislation and tougher rules on the detention of suspects were introduced after the 2005 London transport bombings to crack down on U.K. terrorist operations. The number of intelligence officers at Scotland Yard rose to 1,700, and as many as 3,500 police officers throughout the U.K. were assigned to counterterrorism duties.[5] Thus, the security crackdown

that follows a major attack makes it unlikely that a second attack, and extremely unlikely that a third, could succeed in a short period of time.

Estimating Macro Attack Frequency in the U.S.

The number of planned macro scale attacks feasible in a Western country is thus limited by the austere counterterrorism landscape that terrorists face in organizing a significant number of macro attacks in a given year.[6] The more ambitious the attack mode and the larger the size of a conspiracy, the greater the likelihood of plot disruption by the intelligence services. The more plotters at large, the more connections between them become discernible, and the easier it is for the security services to join the dots and make arrests.

For the U.S., RMS sets a practical operational upper bound for attack frequency of about 10 planned attacks per year, which follows from social network analysis, and is consistent with Western alliance experience in the decade since 9/11. RMS assigns a mean value of 4 for the number of macro planned attacks, which approximates the annual average of macro terrorism plots in the United States.

Since the 9/11 attacks, although the U.S. has incurred many near misses, it has not experienced a successful terrorist attack. Thus, the RMS assignment of 4 for the mean number of macro planned attacks is a conservative estimate. However, over a multi-year time horizon, this element of conservatism is warranted, as the activity rate for future attempted attacks is likely to remain high, as echoed by the late leader Al-Qaeda, Osama bin Laden:

"The new operation of Al-Qaeda has not happened not because we could not penetrate the security measures. It is being prepared and you'll see it in your homeland very soon.[7]*"* ■

Notes and References

1.   Hasan, Suroor, "London 'suicide bombers' were of Pakistani origin," The Hindu, July 14, 2005.

2.   Karon, Tony, Calabresi, Massimo & Thompson, Mark, "Times Square Bomb Arrest Raises U.S. Security Questions," Time, May 5, 2010.

3.   In contrast to the Poisson process used in standard catastrophe modeling, which assumes that events occur independently of one another. In this way, terrorism frequency modeling distinctly differs from standard catastrophe modeling.

4.   Liptak, Adam, "Suspected Leader of 9/11 Attacks Is Said to Confess" New York Times, March 15, 2007.

5.   Gardner, Frank, "One year on: Is the U.K. any safer?" BBC, July 3, 2006.

6.   RMS defines macro terrorism attacks as attacks capable of causing (1) economic losses in excess of $1 billion; (2) more than 100 fatalities or 500 injuries; or (3) massively symbolic damage.

7.   Bergen, Peter, The Osama bin Laden I Know: An Oral History of Al-Qaeda's Leader, Free Press, August 2006, Pg. 200.

7 QUANTIFYING AND MANAGING TERRORISM RISK

At the time, the 9/11 attacks caused the largest insured loss to date, from a peril that was largely unknown to the insurance industry. The attacks led to substantial changes in the industry, bringing about new approaches to underwriting and managing terrorism risk. This chapter summarizes how the insurance industry has changed in the aftermath of the tragic events of 9/11, and offers insight into the approaches to underwriting and managing terrorism risk that have developed in the decade following the attack.

The 9/11 attacks remain the worst terrorist event worldwide in terms of loss to both property and human life, and represent the second-largest U.S. insurance loss in history, exceeded only by Hurricane Katrina in 2005. Insured losses totaled over $40 billion, and were paid out across numerous lines of business, including property, business interruption, workers compensation, auto, life, aviation, liability, and event cancellation. This loss figure does not include compensation for the approximately 10,000 workers whose health was compromised during rescue and clean-up efforts at the World Trade Center site, nor does it represent total economic losses.

Coping in the Aftermath

Prior to the 9/11 attacks, most insurers could not conceive of a terrorism loss as significant as that caused by the attacks on the World Trade Center and Pentagon. Terrorism coverage was not typically excluded from commercial contracts in the U.S., nor was premium explicitly charged to cover the risk. After the attacks, many insurers reacted by excluding terrorism coverage from commercial contracts, throwing the industry into disarray. Commercial property owners could not find adequate coverage at affordable rates, particularly in major metropolitan areas, and construction projects came to a halt as banks began requiring terrorism coverage for funding.

Congress intervened by enacting the Terrorism Risk Insurance Act (TRIA) in November 2002.[1] In exchange for making terrorism insurance available to all policyholders, the government would provide partial coverage for losses resulting from "certified" acts of terrorism.[2] TRIA provided a federal backstop for insurance claims related to terrorism, and was designed as a temporary measure until the insurance industry developed adequate solutions to insure terrorism risk. The placement of TRIA ensured the availability and affordability of terrorism coverage for commercial lines,

and helped the industry recover from 9/11. Since 2002, TRIA has been revised and extended twice, but is due to expire at the end of 2014 unless extended again. However, insurer retentions and pro-rata share of loss have increased substantially over time and coverage is not available for all exposed lines of business, such as group life and homeowners insurance. Therefore, considerable terrorism risk within the insurance market remains.

Shortly after 9/11, a number of countries established public and private terrorism pools to cover losses in the event of a terrorist attack. Eligibility varies by country, but typically includes commercial property and business interruption losses. In some cases, coverage extends to life and health insurers to protect against claims such as health care, life, and disability. Typically, premiums are collected and calculated based on the physical location of the risk, and its associated tier or perceived level of risk.

Policy Changes

Following the 9/11 attacks, the definition of occurrence on most policies became a highly contested issue. Should each plane that crashed into the World Trade Center towers be considered a separate occurrence under the coverage terms of re/insurance policies? The combined insured limit of the World Trade Center towers totaled $3.55 billion, and some policies were required to pay those claims as separate loss occurrences.[3] Today, more specific policy language exists to limit the amount of loss sustained from events comprising multiple attacks by defining an occurrence in less ambiguous terms.

Another major change arising from the 9/11 attacks concerned fire coverage. In the U.S., standard fire policy regulations require that some states provide coverage for loss due to fire regardless of the cause. As of 2002, 31 states mandated these regulations; insurers in these states were required to provide coverage for terrorism-related fire, even for policies that had declined coverage under TRIA.[4] Since then, many states have modified their requirements to allow for the exclusion of terrorism-related fire coverage. Today, only 14 states still require fire coverage for terrorist attacks under the standard fire policy statute. But, New York, California, and other high-risk states are among these 14, leaving many insurers responsible for covering this risk.[5]

The Evolution of Terrorism Risk Management

In the past decade, although relatively few major attacks against Western countries have occurred—and none approaching the magnitude of 9/11—terrorism continues to pose a constant threat. Since 9/11, there have been nearly 40 attempted attacks in the U.S. and over 2,000 successful large-scale attacks worldwide. The lack of a successful attack in the U.S. can be attributed to the improvements in counterterrorism security in the post-9/11 environment. The U.S. has undertaken significant efforts to improve its defense capabilities against future terrorist attacks, and there is a better understanding of terrorists' current operational capabilities. Insurers responded by adopting new technologies and risk models, and by more closely monitoring and managing the risks they cover.

Managing Accumulations

In the aftermath of 9/11, the insurance industry struggled to quantify the frequency and loss potential of terrorism risk. This led to development of simple approaches to quickly identify multi-line exposure concentrations in a confined area. Typically, insurers would define a radius of attack in at-risk areas, and accumulate 100% of the exposed risk within that circular zone. Accumulation zones were differentiated largely by ranking the amount exposed. Zones that exceeded a company-specified threshold were flagged and monitored to maintain an acceptable level of risk.

Insurers soon recognized the need to improve the quality and resolution of their data to improve the accuracy of these estimates, and subsequently moved from coding data at the county, city, or ZIP Code level to focus on address-level data capture. This allowed companies to better manage exposure concentrations within a geographically focused area such as a 400-meter radius. Emphasis was placed on key urban areas and around "trophy" buildings that were at greatest risk of attack. Enhanced capabilities, such as address geocoding at the building level, were introduced and implemented to improve positional accuracy and identify multiple addresses and policies within a single structure. Databases that captured building characteristics to check the accuracy of data and supplement incomplete information were also developed.

The high loss correlation of terrorism across multiple lines of business prompted insurers to capture data and analyze exposures not typically thought to be at risk for catastrophic events, such as workers compensation, life, and disability. This gave rise to the practice of accumulation management to track the aggregate risk across various non-property lines. Workers compensation insurers, in particular, made marked improvements in data capture, and by 2004 had largely moved from mainly capturing payroll at the state-level to capturing the number of employees at a location. Large workers compensation insurers also started to quantify the impacts of other catastrophic events such as earthquakes on their portfolios.

Today, accumulation management is moving toward a more sophisticated, risk-based approach that takes advantage of technological advances such as aerial imagery and geographic information system (GIS) solutions that were typically not commercially available at the time of 9/11. Integrated reporting and mapping capabilities are now commonly used to visualize exposures, accumulation areas, and potential terrorist targets, and to assess relative risk. Insurers can drill into high-risk accumulation zones to efficiently assess just how concentrated the exposure is, and determine the accounts, policies, and locations driving the overall exposure. And, integrated mapping and reporting enables insurers to effectively differentiate accumulation zones by relative risk rather than by exposed risk alone. These capabilities help insurers establish sound underwriting guidelines in areas where terrorists are more likely to attack; understand where to limit the amount of business they write; and identify areas where they could grow their business.

While accumulation management remains a key component of managing terrorism risk, it is considered a conservative method compared to approaches that also assess the potential for loss. Terrorism loss modeling provides a more realistic range of loss compared to exposure management because it takes into account the amount exposed as well as the vulnerability of the locations impacted by the attack.
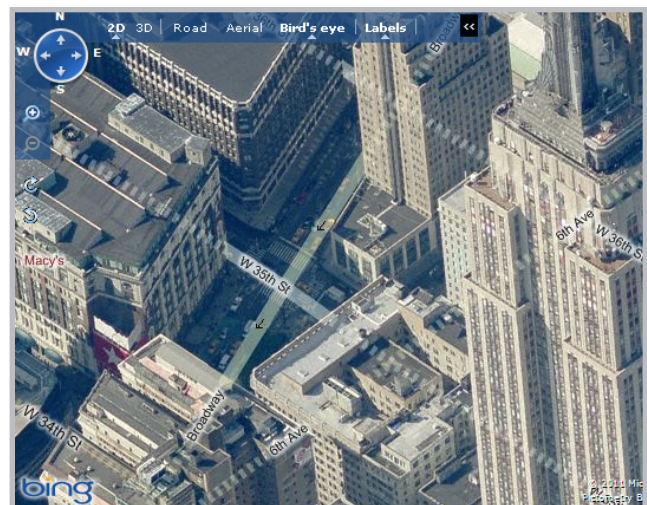
High-resolution aerial imagery is used to visualize targets.

Modeling Terrorism Risk

Since 9/11, insurers have grown increasingly comfortable with using models to manage terrorism risk. While some companies still focus on accumulation management, the industry standard is shifting toward terrorism risk modeling because it offers a more holistic approach to understanding the loss potential of exposure concentrations.

Most insurers now use scenario loss modeling to manage terrorism loss to acceptable loss levels at potential terrorist targets as well as insured locations. Because conventional bomb attacks have a relatively high likelihood of occurrence compared to attack modes such as aircraft hijacking, and can produce significant damage and human injury, bomb attacks serve as the benchmark scenario for scenario loss modeling. Attack scenarios using a 2-ton or 5-ton bomb have become the industry standard, which is driven by the current understanding of the intent and capabilities of terrorist groups.

In the post-9/11 risk environment, scenario loss modeling is also used by regulatory agencies such as A.M. Best, which includes the 5-ton bomb scenario as part of its rating evaluation for property and casualty insurers in its Supplemental Rating Questionnaire (SRQ). Lloyds of London also began including terrorism scenarios as part of its Realistic Disaster Scenarios (RDS) after 9/11.

Probabilistic catastrophe models have been an integral part of the insurance industry's risk management practices for the past several decades; yet, skepticism over the use of probabilistic models to manage terrorism risk remains, largely stemming from the lack of historical terrorism data and the uncertainty in the threat landscape. However, with more empirical evidence and ample literature on the study of terrorism, probabilistic models have moved away from reliance on subjectivity in

Bomb scenario attack footprint

assessing terrorism threat.[6] Today's probabilistic models use social network analysis to assess terrorism threat based on an understanding of how the counterterrorism environment of each country impacts the likelihood of a successful attack. This empirical, analytical process of identifying terrorist social network links has been successful in thwarting all but a few plots against the Western alliance since 9/11, despite the high jihadi threat level. Social network analysis has proven effective in lessening the uncertainty around the frequency of successful terrorist attacks.

RISK MANAGEMENT APPLICATIONS

This shift toward empirical modeling has increased confidence in and acceptance of probabilistic terrorism modeling, and insurers have started to rely more heavily on its output, using model results to inform a range of terrorism risk management decisions.

Risk Selection

Pricing for terrorism coverage has continued to decline and level out across many regions, even within major cities perceived to be at a high risk of attack. Terrorism models have helped underwriters select the best risks for their portfolio by providing an understanding of the relative risk to inform decisions around accepting market prices.

### Insurance and Reinsurance Policies and Treaties

Reinsurers and insurers use model results to evaluate the likelihood of policy and treaty attachment, exhaustion, and expected loss, as well as the impact of coverage exclusions.

Coverage Exclusions

While reinsurance coverage for chemical, biological, radiological, and nuclear (CBRN) attacks has become more readily available, affordable rates for capacity and coverage remain limited. Terrorism models are used to analyze the impact of CBRN attacks on reinsurance structures by taking into account the likelihood of respective CBRN attack modes. The results offer insight into the expected loss compared to the market price.

TRIPRA Analysis

The Terrorism Risk Insurance Program Reauthorization Act (TRIPRA) of 2007 provides reinsurance protection for commercial lines insurers; however, significant risk is retained by insurers below the trigger of $100 million, below the 20% deductible, and within the 15% coinsurance above the deductible. Models allow
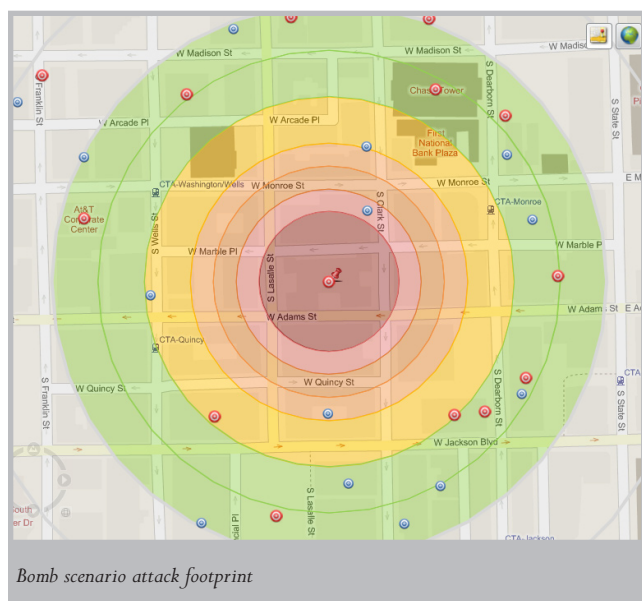
insurers to analyze the impact of TRIPA and evaluate different options for purchasing reinsurance against TRIPRA retention.

Other Risk Transfer Solutions

In addition, probabilistic terrorism models have been used in the securitization of excess mortality risk, to help protect life insurers from extreme losses following a terrorist attack. A number of corporations and entities outside the insurance industry also enlist the help of terrorism models. In 2005, the Congressional Budget Office used the RMS terrorism model to measure the risk transfer effectiveness of TRIA and evaluate different government/insurer sharing options for the Terrorism Risk Insurance Revision and Extension Act.

ENVISIONING THE FUTURE OF TERRORISM RISK MANAGEMENT

Over the past 10 years, the use of loss modeling has become an standard practice for many insurance and reinsurance companies as well as regulatory agencies to assess loss potential across multiple lines of business. As insurer confidence increases with the availability of more empirical data regarding weapon usage and counterterrorism security, it is likely that probabilistic loss modeling will be further integrated into the risk management process.

As global exposure data and geocoding capabilities continue to improve, accumulation and loss control analytics will be implemented across more cities and countries worldwide. Reinsurers and insurers can leverage these region-specific views of terrorism risk to support underwriting and risk management practices for every modeled at-risk nation.

To ensure the best risks are selected for a portfolio, underwriters will gain the technological capability to use real-time analysis for risk monitoring and to assess the impacts of new risks on a portfolio. Terrorism-specific hazard layers such as terrorist targets and relative risk maps will aid insurers in easily understanding potential risk and pricing acceptability.

Insurers will continue to explore risk transfer options for terrorism, and have already begun to use probabilistic risk quantification to secure appropriate coverage. As more detailed questions are asked by rating agencies regarding capital adequacy, companies can use probabilistic model output to account for and respond to their impact on capital after reinsurance under various scenarios. Models can also be used to help insurers derive comparable benchmarks to ensure that capital allocation is efficient and allocated more equally across the range of perils covered by an insurer. Reinsurers can leverage models to gain a view into the relativities between different cedants and different reinsurance structures.

The sheer number of interdicted terrorist plots in the U.S. in the decade since 9/11 demonstrates that while the nature of the threat may change, terrorism risk will remain. As the terrorism landscape evolves, and modeling and data enhancement technology improve, the insurance market will continue to evaluate and leverage the tools available to manage risk from the global terrorism threat. ■

Notes and References

1. *For more information on the Terrorism Risk Insurance Act (TRIA), see the U.S. Treasury website: http://www.treasury.gov/resource-center/fin-mkts/Pages/program.aspx.*

2. *When enacted, a TRIA-certified event was defined as an event causing at least $5 million in aggregate property and casualty insurance losses, be committed by or on behalf of a foreign person or interest to coerce or influence U.S. policy, and take place on U.S. soil.*

3. *Grossi, Patricia, "Property Damage and Insured Losses from the 2001 World Trade Center Attacks," Peace Economics, Peace Science and Public Policy: Vol. 15: Iss. 2, Article 3, 2009.*

4. *The Marsh Report: Terrorism Risk Insurance 2010, Marsh, 23 June 2010, http://insurancemarketreport.com/terrorism2010/Home/tabid/7396/Default.aspx, (accessed on June 20, 2011).*

5. *Ibid.*

6. *For more information on the study of terrorism and the use of models to quantify the risk, see Estimating Terrorism Risk by Henry H. Willis, Andrew R. Morral, Terrence K. Kelly and Jamison Jo Medby, RAND Corporation, 2005; Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection by Henry H. Willis, Tom LaTourrette, Terrence K. Kelly, Scot Hickey, and Samuel Neill, RAND Corporation, 2007; and Guiding Resource Allocations Based on Terrorism Risk by Henry H. Willis, Risk Analysis, v. 27, no. 3, June 2007, pg. 597-606.*

8 CONCLUDING REMARKS

Although the U.S. still faces a significant threat from Al-Qaeda and its affiliates, a decade after 9/11, the nature of this threat has evolved significantly. The 9/11 attacks changed the terrorism landscape, acting as a catalyst upon the key factors driving risk—the threat, the target's vulnerability, and the consequences of a successful attack. The chapters in this report have focused on these risk drivers, presenting RMS' view on the evolution, current state, and future of terrorism risk, which is summarized below.

The Nature of the Threat

Despite being the most hunted terrorist group in the world today, Al-Qaeda and its affiliates continue to dictate the tempo of global terrorism activity. According to RMS research, since 2002, nearly 40 plots inspired by or connected to Al-Qaeda have occurred in the United States, an average of just over 4 a year.

Since 9/11, U.S. foreign policy strategy, particularly regarding the U.S. military presence in Iraq, has placed the U.S. and its allies at greater peril. U.S. policy has alienated a sizeable proportion of the global Muslim community, serving to increase the ranks of Al-Qaeda recruits willing to wage attacks against the United States. In accordance, the Al-Qaeda threat in the U.S. has become much more diverse. The Al-Qaeda core leads the post 9/11 Salafi-jihadist movement, which has inspired Salafi-jihadists to attack the U.S. for religious purposes, and incited the rise of "homegrown" U.S. jihadi terrorists. The U.S. is now at risk of attack from multiple fronts—the Al-Qaeda core, its affiliates, and homegrown terrorists.

Intent versus Capability

Al-Qaeda's intent to attack the U.S. remains strong. However, threat is a function of both intent as well as capability, and the group has faced significant operational and strategic setbacks over the past decade, culminating in the assassination of Osama bin Laden.

Despite these setbacks, Al-Qaeda continues to train and place operatives in the U.S. to carry out smaller yet still deadly plots. And, the group's intent to inflict a mass casualty attack on the U.S. remains strong, as evidenced by its ongoing attempts to acquire chemical, biological, radiological, and nuclear (CBRN) weapons. Although its capability to do so has diminished from that of a decade ago, Al-Qaeda's pursuit of a CBRN arsenal has yet to abate because of the potential for "spectacular," high-severity

outcomes that cannot be produced by conventional attacks. RMS research indicates that Al-Qaeda will be relentless in its pursuit and will someday overcome its capability constraints, making the likelihood of a CBRN attack a matter not of "if," but "when."

The Role of Counterterrorism

Over the past decade, counterterrorism agencies across the globe have played a crucial role in quelling the terrorism threat. RMS analysis of the terrorism landscape has found that in the decade since 9/11, the terrorism threat has largely been balanced by the counterterrorism opposition. As nature of the threat evolves, security forces have been enhanced to meet the threat. This is particularly in the case of the U.S., where the government has responded to shifts in the threat landscape by providing consistent government investment, sound intelligence sharing, and effective counterterrorism policies. These efforts have helped to constrain the capability of Al-Qaeda and its affiliated groups to mount successful attacks in America. Thus, while attack attempt frequency is unlikely to diminish the effective counterterrorism action will help to thwart most macro terror plots.

Modeling and Managing Terrorism Risk

Over the past 10 years, insurers and reinsurers have become more comfortable using loss models to manage terrorism risk. Insurers manage terrorism accumulations using realistic scenarios and event-specific footprints to monitor exposure across multiple lines of business, and probabilistic terrorism models are increasingly used in standard risk management practices. The wealth of research and development on terrorism risk now available has enabled probabilistic terrorism models to shift from a reliance on expert opinion to an objective methodology to assess the terrorism threat, including using social network analysis as a key element in modeling terrorist attack frequency. ■

ACKNOWLEDGMENTS

R I S K   M A N A G E M E N T
S O L U T I O N S ,   I n c .

7575 Gateway Blvd.
Newark, CA 94560
USA

Tel 1.510.505.2500
Fax 1.510.505.2501
Tel 44.20.7444.7600 (Europe)

W O R L D   W I D E   W E B
http://www.rms.com

E M A I L
info@rms.com