HOW TO TRAVEL SAFELY

A STRATFOR GUIDE
TO SECURITY WHILE ABROAD
Contents

Introduction v
A Note on Content vii

The Case for Screening Air Passengers Rather than Belongings 1
Convergence: The Challenge of Aviation Security 3
Airline Security: Gentle Solutions to a Vexing Problem 10
Visa Security: Getting Back to the Basics 15
A Primer on Situational Awareness 23
Terrorism, Vigilance and the Limits of the War on Terror 31
How to Respond to Terrorism Threats and Warnings 36
Aviation Security Threats and Realities 43
The Moscow Attack and Airport Security 49
Travel and Security Risks over Spring Break in Mexico 54
Preparing to Travel Safely 63
Air Travel Security 66
Hotel Security 70
Public Transportation Security 74
Mitigating the Threat of Street Crime 79
## CONTENTS

Protecting Sensitive Information in Electronic Devices When Traveling 83
Common Sense When Traveling Abroad 88
Security During Adventure Travel 92
INTRODUCTION

In order to fully understand a place and its people, a person must go and walk the streets, talk with locals and experience what daily life is truly like. It is difficult to grasp what makes a place unique without experiencing the environment firsthand. Traveling can be an exciting and educational experience regardless of whether the trip is domestic or international, business or personal. However, traveling offers several challenges inherent in leaving one’s comfort zone and going to unfamiliar places with unfamiliar customs.

Security when traveling abroad has changed much in the years since the 9/11 attacks. When trying to board an aircraft or cross an international border, travelers are subjected to security checks more comprehensive — and sometimes invasive — than ever before. Nevertheless, when travelers arrive at their destinations, age-old security issues persist. In addition to the possibility of terrorist attacks or kidnapping, travelers face the far more common threat of crimes such as robbery, assault, property theft or scams.

Some destinations are more dangerous than others, especially when a traveler lacks local knowledge. A traveler may not speak the local language or know where to go or whom to approach in an emergency. Different types of travel, such as adventure travel, have even more specific security issues. It is thus important for a traveler to learn as much as possible about a location before visiting and be prepared for potential dangers. Planning and practice help travelers understand the risks inherent to travel and reduce anxiety associated with being in unfamiliar territory.
Personal security, such as knowing how to keep a low profile to avoid attracting criminals’ notice, also is important, as is ensuring adequate security of property. Many a trip has been ruined by a stolen passport or credit card. This is especially true on business trips, where travelers must also be vigilant of potential threats to their company’s proprietary information. Laptops and important information can be protected, but in order to do so a business traveler must first understand from whence potential threats can come.

While savvy travelers will be aware of these threats, they also understand that constant agitation and paranoia are counterproductive, both to enjoyment of the experience and to their own security. Travel security is not about constantly looking for threats; it is about maintaining proper situational awareness and understanding the risks involved with being in a foreign location.

The best defense against any travel security risks is awareness of their existence, followed by preparation, practice and a healthy dose of common sense. This book has collected several STRATFOR reports detailing how a traveler can keep oneself safe when abroad.

STRATFOR
Austin, Texas
Oct. 27, 2011
A NOTE ON CONTENT

STRATFOR presents the following reports as they originally appeared on our subscription website, www.STRATFOR.com. These pieces represent some of our best tutorials related to travel security since August 2006, presented in the order in which they were published. Since most of the articles were written as individual analyses, there may be overlap from piece to piece and chapter to chapter, and some of the information may seem dated. Naturally, some observations are linked to a specific time or event years removed from today’s security environment, which continues to evolve, but the recommendations and principles are every bit as relevant today as they were when they were written.
The Case for Screening Air Passengers Rather than Belongings

*X August 18, 2006*

Irish airline Ryanair issued an ultimatum to the British government Aug. 18 to restore normal airport security measures within a week or risk being sued by the company for compensation. Ryanair said it faces more than $3.7 million in losses from disrupted flight schedules in the aftermath of the plot to destroy aircraft in flight using liquid explosives. In announcing the foiled plot Aug. 10, the British government immediately banned passengers from bringing carry-on luggage and liquids of all kinds aboard planes originating in the United Kingdom.

Liquid explosives do pose a serious threat to airliners in flight, although a review of previous plots against planes indicates these types of explosives are not the only thing security services need to be concerned about. Moreover, militants can be expected to adapt to evolving airline security measures.

The British case is reminiscent of Operation Bojinka, a plot to use a modular explosive device made of a doll stuffed with nitrocel lulose and augmented by a bottle of liquid explosive. North Korean agents used liquid explosive PLX, disguised as a fifth of liquor, to destroy KAL Flight 858 in 1987. A number of other powerful, commercially manufactured liquid explosives also could be used to attack an airliner, such as nitroglycerine and Astrolite. Improvised versions of these explosives also can be manufactured.

Creative bombmakers have hidden explosives in a number of imaginative ways, perhaps most notably the Popular Front for the
Liberation of Palestine-General Command (PFLP-GC), which did some outside-the-box thinking when it melted the explosives TNT and Composition B and cast them into a variety of shapes, including a tea set. PFLP-GC also hid Semtex and other plastic explosives in a variety of items, including running shoes and electronics.

In fact, electronics also have been a popular choice for bombmakers looking to smuggle an improvised explosive device (IED) aboard planes. Perhaps the most famous case is the Libyan-constructed device concealed inside a Toshiba radio cassette player that was used to bring down Pan Am Flight 103. Similar devices hidden in another model of Toshiba cassette player were found in a raid on a PFLP-GC safe house in Germany a few months before the Pan Am 103 bombing.

In the 1987 KAL case, the firing train and a small charge of C-4 hidden inside the radio were used to initiate the PLX. In a London case in 1986, Nezar Hindawi, a Jordanian who later acknowledged working for Syrian intelligence, gave his unwitting and pregnant Irish girlfriend an IED concealed in bag to take on an El Al flight from London to Tel Aviv. The timer and detonator for the device were concealed in a pocket calculator. El Al security detected the device before it could be taken aboard the plane, and Hindawi was quickly arrested. In 1996, Israelis used an IED concealed in a cell phone to assassinate Yahya Ayyash, aka “The Engineer,” an infamous Hamas bombmaker.

These are only past IED incidents involving airplanes, though it is important to point out that, as security measures change, terrorist tactics also will adapt, much as narcotics “mules” have adapted to efforts to prevent them from bringing narcotics aboard planes by using everything from body cavities to dead babies.

In addition to Richard Reid’s infamous shoe bomb, there are many other ways in which explosives could be “worn” onto a plane. In the bombing of Philippine Airlines Flight 434, Abdel Basit and his associates used nitrocellulose camouflaged inside a doll, though nitrocellulose also could be easily hidden in any number of clothing items that have fiber filling, such as mittens and winter coats. Additionally, the design of the ubiquitous suicide vests and belts could allow explosives
to be walked through a magnetometer if all the metal components were removed. In August 2004, Israeli authorities found explosive underwear on a young Palestinian attempting to enter Israel at the Erez border crossing. Because of the Reid plot, all passengers must remove their shoes. Had the Palestinian been attempting to board a plane, there is no telling how the incident would now affect passengers at airline security checkpoints.

It is virtually impossible to use technical screening measures to absolutely prevent explosive material from being brought on board an aircraft. Prison authorities using magnetometers and strip searches have failed to completely prevent all contraband from slipping through. The need for a greater reliance on other methods — such as name checks, interviews and behavioral profiling — to keep airplanes safe seems apparent.

Convergence: The Challenge of Aviation Security

September 16, 2009

On Sept. 13, As-Sahab media released an audio statement purportedly made by Osama bin Laden that was intended to address the American people on the anniversary of the 9/11 attacks. In the message, the voice alleged to be that of bin Laden said the reason for the 9/11 attacks was U.S. support for Israel. He also said that if the American people wanted to free themselves from “fear and intellectual terrorism,” the United States must cut its support for Israel. If the United States continues to support Israel, the voice warned, al Qaeda would continue its war against the United States “on all possible fronts” — a not so subtle threat of additional terrorist attacks.

Elsewhere on Sept. 14, a judge at Woolwich Crown Court in the United Kingdom sentenced four men to lengthy prison sentences for their involvement in the disrupted 2006 plot to destroy multiple aircraft over the Atlantic using liquid explosives. The man authorities
claimed was the leader of the cell, Abdulla Ahmed Ali, was sentenced to serve at least 40 years. The cell’s apparent logistics man, Assad Sarwar, was sentenced to at least 36 years. Cell member Tanvir Hussain was given a sentence of at least 32 years and cell member Umar Islam was sentenced to a minimum of 22 years in prison.

The convergence of these two events (along with the recent release of convicted Pan Am 103 bomber Abdel Basset Ali al-Megrahi and the amateurish Sept. 9 hijacking incident in Mexico using a hoax improvised explosive device [IED]) has drawn our focus back to the topic of aviation security — in particular, IED attacks against aircraft. As we weave the strands of these independent events together, they remind us not only that attacks against aircraft are dramatic, generate a lot of publicity and can cause very high body counts (9/11), but also that such attacks can be conducted simply and quite inexpensively with an eye toward avoiding preventative security measures (the 2006 liquid-explosives plot.)

Additionally, while the 9/11 anniversary reminds us that some jihadist groups have demonstrated a fixation on attacking aviation targets — especially those militants influenced by the operational philosophies of Khalid Sheikh Mohammed (KSM) — the convictions in the 2006 plot highlight the fact that the fixation on aviation targets lives on even after the 2003 arrest of KSM.

In response to this persistent threat, aviation security has changed dramatically in the post-9/11 era, and great effort has been undertaken at great expense to make attacks against passenger aircraft more difficult. Airline attacks are harder to conduct now than in the past, and while many militants have shifted their focus to easier targets like subways or hotels, there are still some jihadists who remain fixated on the aviation target, and we undoubtedly will see more attempts against passenger aircraft — in spite of the restrictions on the quantities of liquids that can be taken aboard aircraft and the now mandatory shoe inspections.

Quite simply, militants will seek alternate ways to smuggle components for IEDs aboard aircraft. This is where another thread comes in — that of the Aug. 28 assassination attempt against Saudi Deputy
Interior Minister Prince Mohammed bin Nayef. The tactical innovation employed in this attack highlights the vulnerabilities that still exist in airline security.

**Shifts**

The airline security paradigm changed on 9/11. In spite of the recent statement by al Qaeda leader Mustafa Abu al-Yazid that al Qaeda retains the ability to conduct 9/11-style attacks, his boast simply does not ring true. After the 9/11 attacks, there is no way a captain and crew (or a group of passengers for that matter) are going to relinquish control of an aircraft to hijackers armed with box-cutters — or even a handgun or IED. A commercial airliner will never again be commandeered from the cockpit and flown into a building — especially in the United States.

Because of the shift in mindset and improvements in airline security, the militants have been forced to alter their operational framework. In effect, they have returned to the pre-9/11 operational concept of taking down an aircraft with an IED rather than utilizing an aircraft as human-guided missile. This return was first demonstrated with the December 2001 attempt by Richard Reid to destroy American Airlines Flight 63 over the Atlantic with a shoe bomb, and later by the thwarted 2006 liquid-explosives plot. The operational concept in place now is clearly to destroy rather than commandeer. Both the Reid plot and the 2006 liquid-bomb plot show links back to the operational philosophy evidenced by Operation Bojinka in the mid-1990s, which was a plot to destroy multiple aircraft in flight over the Pacific Ocean.

The return to Bojinka principles is significant because it represents not only an IED attack against an aircraft but also a specific method of attack: a camouflaged, modular IED that the bomber smuggles onto an aircraft in pieces and then assembles once he or she is aboard and well past security. The original Bojinka plot used baby dolls to smuggle the main explosive charge of nitrocellulose aboard the aircraft. Once on the plane, the main charge was primed with an
improvised detonator that was concealed inside a carry-on bag and then hooked into a power source and a timer (which was disguised as a wrist watch). The baby-doll device was successfully smuggled past security in a test run in December 1994 and was detonated aboard Philippine Air Flight 434.

The main charge in the baby-doll devices, however, proved insufficient to bring down the aircraft, so the plan was amended to add a supplemental charge of liquid triacetone triperoxide (or TATP, aptly referred to as “Mother of Satan”), which was to be concealed in a bottle of contact lens solution. The plot unraveled when the bomb-maker, Abdel Basit (who is frequently referred to by one of his alias names, Ramzi Yousef) accidentally set his apartment on fire while brewing the TATP.

The Twist

The 2006 liquid-bomb plot borrowed the elements of using liquid explosives and disguised individual components and attacking multiple aircraft at the same time from Bojinka. The 2006 plotters sought to smuggle their liquid explosives aboard using drink bottles, instead of contact lens solution containers, and planned to use different types of initiators. The biggest difference between Bojinka and more recent plots is that the Bojinka operatives were to smuggle the components aboard the aircraft, assemble the IEDs inside the lavatory and then leave the completed devices hidden aboard multi-leg flights while the operatives got off the aircraft at an intermediate stop. The more recent iterations of the jihadist airplane-attack concept, including Richard Reid’s attempted shoe bombing and the 2006 liquid-bomb plot, planned to use suicide bombers to detonate the devices mid-flight. The successful August 2004 twin aircraft bombings in Russia by Chechen militants also utilized suicide bombers.

The shift to suicide operatives is not only a reaction to increased security but also the result of an evolution in ideology: Suicide bombings have become more widely embraced by jihadist militants than they were in the early 1990s. As a result, the jihadist use of suicide
bombers has increased dramatically in recent years. The success and glorification of suicide operatives, such as the 9/11 attackers, has been an important factor in this ideological shift.

One of the most recent suicide attacks was the Aug. 28 attempt by al Qaeda in the Arabian Peninsula (AQAP) to assassinate Saudi Prince Mohammed bin Nayef. In that attack, a suicide operative smuggled an assembled IED containing approximately one pound of high explosives from Yemen to Saudi Arabia concealed in his rectum. While in a meeting with Mohammed, the bomber placed a telephone call and the device hidden inside him detonated.

In an environment where militant operational planning has shifted toward concealed IED components, this concept of smuggling components such as explosive mixtures inside of an operative poses a daunting challenge to security personnel — especially if the components are non-metallic. It is one thing to find a quantity of C-4 explosives hidden inside a laptop that is sent through an X-ray machine; it is quite another to find that same piece of C-4 hidden inside someone’s body. Even advanced body-imaging systems like the newer backscatter and millimeter wave systems being used to screen travelers for weapons are not capable of picking up explosives hidden inside a person's body. Depending on the explosive compounds used and the care taken in handling them, this method of concealment can also present serious challenges to explosive residue detectors and canine explosive detection teams. Of course, this vulnerability has always existed, but it is now highlighted by the new tactical reality. Agencies charged with airline security are going to be forced to address it just as they were previously forced to address shoe bombs and liquid explosives.

Actors

Currently, there are three different actors in the jihadist realm. The first is the core al Qaeda group headed by bin Laden and Ayman al-Zawahiri. The core al Qaeda organization has been hit hard over the past several years, and its operational ability has been greatly
diminished. It has been several years since the core group has conducted a spectacular terror attack, and it has focused much of its effort on waging the ideological battle as opposed to the physical battle.

The second group of actors in the jihadist realm involves the regional al Qaeda franchise groups or allies, such as al Qaeda in the Arabian Peninsula, Jemaah Islamiyah and Lashkar-e-Taiba. These regional jihadist groups have conducted many of the most spectacular terrorist attacks in recent years, such as the November 2008 Mumbai attacks and the July 2009 Jakarta bombings.

The third group of actors is the grassroots jihadist militants, who are essentially do-it-yourself terrorist operatives. Grassroots jihadists have been involved in several plots in recent years, including suicide bomb plots in the United States and Europe.

In terms of terrorist tradecraft such as operational planning and bomb-making, the core al Qaeda operatives are the most advanced, followed by the operatives of the franchise groups. The grassroots operatives are generally far less advanced in terms of their tradecraft. However, any of these three actors are capable of constructing a device to conduct an attack against an airliner. The components required for such a device are incredibly simple — especially so in a suicide attack where no timer or remote detonator is required. The only components required for such a simple device are a main explosive charge, a detonator (improvised or otherwise) and a simple initiator such as a battery in the case of an electric detonator or a match or lighter in the case of a non-electric detonator.

The October 2005 incident in which a University of Oklahoma student was killed by a suicide device he was carrying demonstrates how it is possible for an untrained person to construct a functional IED. However, as we have seen in cases like the July 2005 attempted attacks against the London Underground and the attempted strikes in July 2007 against nightclubs in London and the airport in Glasgow, grassroots operatives also can botch things, due to a lack of technical bomb-making ability. Nevertheless, the fact remains that constructing IEDs is actually easier than effectively planning an attack and successfully executing it.
Getting a completed device or its components by security and onto the aircraft is a significant challenge, but as we have discussed, it is possible to devise ways to overcome that challenge. This means that the most significant weakness of any suicide-attack plan is the operative assigned to conduct the attack. Even in a plot to attack 10 or 12 aircraft, a group would need to manufacture only about 12 pounds of high explosives — about what is required for a single, small suicide device and far less than is required for a vehicle-borne explosive device. Because of this, the operatives are more of a limiting factor than the explosives themselves, as it is far more difficult to find and train 10 or 12 suicide bombers.

A successful attack requires operatives not only to be dedicated enough to initiate a suicide device without getting cold feet; they also must possess the nerve to calmly proceed through airport security checkpoints without alerting officers that they are up to something sinister. This set of tradecraft skills is referred to as demeanor, and while remaining calm under pressure and behaving normally may sound simple in theory, practicing good demeanor under the extreme pressure of a suicide operation is very difficult. Demeanor has proven to be the Achilles’ heel of several terror plots, and it is not something that militant groups have spent a great deal of time teaching their operatives. Because of this, it is frequently easier to spot demeanor mistakes than it is to find well-hidden explosives.

In the end, it is impossible to keep all contraband off aircraft. Even in prison systems, where there is a far lower volume of people to screen and searches are far more invasive, corrections officials have not been able to prevent contraband from being smuggled into the system. Narcotics, cell phones and weapons do make their way through prison screening points. Like the prison example, efforts to smuggle contraband aboard aircraft can be aided by placing people inside the airline or airport staff or via bribery. These techniques are frequently used to smuggle narcotics on board aircraft.

Obviously, efforts to improve technical methods to locate IED components must not be abandoned, but the existing vulnerabilities in airport screening systems demonstrate that emphasis also needs
to be placed on finding the bomber and not merely on finding the bomb. Finding the bomber will require placing a greater reliance on other methods such as checking names, conducting interviews and assigning trained security officers to watch for abnormal behavior and suspicious demeanor. It also means that the often overlooked human elements of airport security — including situational awareness, observation and intuition — need to be emphasized now more than ever.

Airline Security: Gentle Solutions to a Vexing Problem

January 13, 2010

U.S. President Barack Obama outlined a set of new policies Jan. 7 in response to the Dec. 25, 2009 Northwest Airlines bombing attempt, which came the closest to a successful attack on a U.S. flight since Richard Reid’s failed shoe-bombing in December 2001. As in the aftermath of that attempt, a flurry of accusations, excuses and policy prescriptions have emanated from Washington since Christmas Day concerning U.S. airline security. Whatever changes actually result from the most recent bombing attempt, they will likely be more successful at pacifying the public and politicians than preventing future attacks.

At the heart of President Obama’s policy outline were the following key tactics: pursue enhanced screening technology in the transportation sector, review the visa issuance and revocation process, enhance coordination among agencies for counterterrorism (CT) investigations and establish a process to prioritize such investigations. While such measures are certainly important, they will not go far enough, by themselves, to meaningfully address the aviation security challenges the United States still faces almost nine years after 9/11.
Holes in the System

For one thing, technology must not be seen as a panacea. It can be a very useful tool for finding explosive devices and weapons concealed on a person or in luggage, but it is predictable and reactive. In terms of aviation security, the federal government has consistently been fighting the last war and continues to do so. Certain practical and effective steps have been taken. Hardening the cockpit door, deploying air marshals and increasing crew and passenger awareness countered the airline hijacking threat after 9/11; requiring passengers to remove their shoes and scanning them prior to boarding followed Reid’s 2001 shoe-bombing attempt; and restrictions on liquids and gels followed the 2006 trans-Atlantic plot. Not enacting these measures would have meant not learning from past mistakes, and they do ensure that unsophisticated “copycat” attackers are not successful. But such measures — even those that are less technological — fail to take into account innovative militants, who are eager and able to exploit inevitable weaknesses in the process.

Even advanced body-imaging systems like the newer backscatter and millimeter-wave systems now being used to screen travelers cannot pick up explosives hidden inside a person’s body using condoms or tampons — a tactic that was initially thought to have been used in the Aug. 28 assassination attempt against Saudi Deputy Interior Minister Prince Mohammed bin Nayef. (It is now believed that the attacker in that case used an underwear bomb like the one used in the Christmas Day attempt.) Moreover, X-ray systems cannot detect explosives cleverly disguised in carry-on baggage or smuggled past security checkpoints — something that drug smugglers routinely do.

Preventing attacks against U.S. airliners would require unrealistically invasive and inconvenient measures that the airline industry and American society are simply not prepared to implement. El Al, Israel’s national airline, is one international carrier that conducts thorough searches of every passenger and every handbag, runs checked luggage through a decompression chamber and has two air marshals on each flight. The airline also refuses to let some people (including many
Muslims) on board. While these practices have been successful in preventing terrorist attacks against the airline, they are not in line with American and European culture and President Obama’s insistence that measures remain consistent with privacy rights and civil liberties. It is also economically and politically unfeasible for major U.S. airlines operating hundreds of flights per day from hundreds of different cities to impose measures such as those followed by El Al, an airline with fewer planes and a smaller area of operation.

And as long as U.S. airport security relies on screening techniques that are only moderately invasive, there will be holes that innovative attackers will be able to exploit. While screening technology is advancing, there is nothing in the foreseeable future that would be able to do more screening with less invasiveness. The U.S. prison system grapples with the same problem, and even there, where inmates are searched far more invasively than air travelers, contraband is still able to flow into facilities.

Focusing on the visa issuance and revocation process also leaves holes in the system. The Christmas Day bomber, Umar Farouk Abdulmutallab, had been given a multiple-entry U.S. visa, which allowed him to travel to the United States. When Abdulmutallab’s father expressed concerns to officials at the U.S. Embassy in Abuja, Nigeria, on Nov. 19, 2009, that his son might have been involved with Yemen-based Islamist militants, Abdulmutallab’s name and passport number were sent from the U.S. Embassy in Abuja to Washington and placed in the “Visa Viper” system, which specifically pertains to visas and terrorist suspects. His name and passport number were also logged into the Terrorist Identities Datamart Environment, but not the “no-fly” list.

This standard operating procedure (which does not automatically result in a visa revocation) passed the responsibility from the CIA agents who spoke to Abdulmuttalab’s father on to the U.S. State Department, where agents unfamiliar with the specifics of the case did not, apparently, decide to act on it. In hindsight, the decision not to take the father’s warning more seriously appears to be a glaring mistake, but in context it seems less obvious. The father’s tip was
vague, with little indication of what his son was up to or, more important to U.S. CT agents, that he was planning even to travel to the United States, much less attack a U.S. airliner.

**Intelligence Limitations**

The possibility of yet another jihadist suspect emerging in the Middle East does not pose an existential threat to the United States, so this raises the third challenge: prioritizing CT investigations. Vague warnings such as the tip from Abdulmuttalab’s father spring up constantly throughout the world and CT investigators have to prioritize them. Only the most serious cases get assigned to an investigator to follow up on while the rest are filed away for future reference. If the same name pops up again with more information on the threat, then more action is taken. U.S. CT agents are most concerned about specific threats to the United States, and with no actionable intelligence that Abdulmutallab was plotting an attack against the United States, his case was given a lower priority.

Nevertheless, not acting immediately on the father’s vague threat proved to be a near-fatal move. This highlights the danger of the unsophisticated, ill-trained militant, referred to in U.S. CT circles as a “Kramer jihadist” (after the bumbling character in the sitcom “Seinfeld”). By himself, a Kramer jihadist poses a minimal threat, but when combined with a trained operative or group, he can become a formidable weapon. Abdulmutallab had been radicalized, but there is nothing to suggest that he had extensive jihadist training or any tactical expertise. He was simply a willing agent with a visa to the United States. When put in the hands of a competent, well-trained operator (such as those involved with al Qaeda in the Arabian Peninsula), a Kramer jihadist can be outfitted with a device and given a support network that could supply him with transportation and direction to carry out an effective attack. There are simply too many radical Islamists in the world to investigate each one, but immediately revoking visas to keep suspects off U.S. airliners until they can be
investigated further is a fairly simple process and would be an effective deterrent.

Finally, the lack of coordination among agencies in CT investigations is an old problem that dates back well before 9/11. This challenge lies in the fact that the U.S. intelligence community is broken up into specific agencies — each with its own specific jurisdiction and incentive to leverage its power in Washington by controlling the flow of information. This system ensures that no single agency becomes too powerful and self-interested, but it also fractures the intelligence community and bureaucratizes intelligence sharing.

**National Counterterrorism Center**

In order to investigate a case like Abdulmutallab’s, agents from the CIA must work with agents from the FBI, and the State Department is tasked with coordinating the requests for information from various foreign governments (whose information is not always reliable). For foreign threats specifically aimed at airlines, agents from the Transportation Security Administration, Federal Aviation Administration, Office of Director of National Intelligence, and Immigration and Customs Enforcement must be notified. Rallying and coordinating all the appropriate actors and agencies to respond to a threat requires careful bureaucratic maneuvering and presents numerous opportunities to be bogged down at every step. Certainly, the more overt the threat, the easier it is to move the bureaucracy, but a case as opaque as Abdulmutallab’s would not likely inspire a quick and decisive follow-up.

The U.S. National Counterterrorism Center (NCTC) was created to aggregate threats from various local, state and federal agencies all over the world in order to streamline the threat-identification and investigation process. However, the additional bureaucracy that was generated with the formation of the NCTC has essentially canceled out any benefit that the center might have contributed.

When it comes down to it, modern airliners — full of people and fuel — are extremely vulnerable targets that can produce highly
dramatic carnage, characteristics that attract militants and militant groups seeking global notoriety. And Abdulmutallab’s efforts on Christmas Day certainly will not be the last militant attempt to bring an airliner down. As security measures are changed in response to this most recent attempt, terrorist planners will be watching closely and are sure to adapt their tactics accordingly.

---

**Visa Security: Getting Back to the Basics**

*February 18, 2010*

Usually in the STRATFOR Global Security and Intelligence Report, we focus on the tactical details of terrorism and security issues in an effort to explain those issues and place them in perspective for our readers. Occasionally, though, we turn our focus away from the tactical realm in order to examine the bureaucratic processes that shape the way things run in the counterterrorism, counterintelligence and security arena. This look into the struggle by the U.S. government to ensure visa security is one of those analyses.

As STRATFOR has noted for many years now, document-fraud investigations are a very useful weapon in the counterterrorism arsenal. Foreigners who wish to travel to the United States to conduct a terrorist attack must either have a valid passport from their country of citizenship and a valid U.S. visa, or just a valid passport from their home country if they are a citizen of a country that does not require a visa for short-term trips (called visa-waiver countries).

In some early jihadist attacks against the United States, such as the 1993 World Trade Center bombing, the operatives dispatched to conduct the attacks made very clumsy attempts at document fraud. In that case, the two operational commanders dispatched from Afghanistan to conduct the attack arrived at New York’s Kennedy Airport after having used photo-substituted passports (passports where the photographs are literally switched) of militants from visa-waiver countries.
who died while fighting in Afghanistan. Ahmed Ajaj (a Palestinian) used a Swedish passport in the name of Khurram Khan, and Abdul Basit (a Pakistani also known as Ramzi Yousef) used a British passport in the name of Mohamed Azan. Ajaj attempted to enter through U.S. Immigration at Kennedy Airport using the obviously photo-substituted passport and was arrested on the spot. Basit used the altered British passport to board the aircraft in Karachi, Pakistan, but upon arrival in New York he used a fraudulently obtained but genuine Iraqi passport in the name of Ramzi Yousef to claim political asylum and was released pending his asylum hearing.

But the jihadist planners learned from amateurish cases like Ajaj’s and that of Ghazi Ibrahim Abu Mezer, a Palestinian who attempted to conduct a suicide attack against the New York subway system. U.S. immigration officials arrested him on three occasions in the Pacific Northwest as he attempted to cross into the United States illegally from Canada. By the Millennium Bomb Plot in late 1999, Ahmed Ressam, an Algerian who initially entered Canada using a photo-substituted French passport, had obtained a genuine Canadian passport using a fraudulent baptismal certificate. He then used that genuine passport to attempt to enter the United States in order to bomb Los Angeles International Airport. Ressam was caught not because of his documentation but because of his demeanor — and an alert customs inspector prevented him from entering the country.

So by the time the 9/11 attacks occurred, we were seeing groups like al Qaeda preferring to use genuine travel documents rather than altered or counterfeit documents. Indeed, some operatives, such as Ramzi bin al-Shibh, a Yemeni, were unable to obtain U.S. visas and were therefore not permitted to participate in the 9/11 plot. Instead, bin al-Shibh took on a support role, serving as the communications cutout between al Qaeda’s operational planner, Khalid Sheikh Mohammed, and al Qaeda’s tactical commander for the operation, Mohamed Atta. It is important to note, however, that the 19 9/11 operatives had obtained a large assortment of driver’s licenses and state identification cards, many of them fraudulent. Such documents are far easier to obtain than passports.
After the Sept. 11 attacks and the 9/11 Commission report, which shed a great deal of light on the terrorist use of document fraud, the U.S. government increased the attention devoted to immigration fraud and the use of fraudulent travel documents by terrorist suspects. This emphasis on detecting document fraud, along with the widespread adoption of more difficult to counterfeit passports and visas (no document is impossible to counterfeit), has influenced jihadists, who have continued their shift away from the use of fraudulent documents (especially poor quality documents). Indeed, in many post-9/11 attacks directed against the United States we have seen jihadist groups use U.S. citizens (Jose Padilla and Najibullah Zazi), citizens of visa-waiver countries (Richard Reid and Abdulla Ahmed Ali), and other operatives who possess or can obtain valid U.S. visas such as Umar Farouk Abdulmutallab. These operatives are, for the most part, using authentic documents issued in their true identities.

Concerns expressed by the 9/11 Commission over the vulnerability created by the visa-waiver program also prompted the U.S. government to establish the Electronic System for Travel Authorization (ESTA), which is a mandatory program that prescreens visa-waiver travelers, including those transiting through the United States. The ESTA, which became functional in January 2009, requires travelers from visa-waiver countries to apply for travel authorization at least 72 hours prior to travel. This time period permits the U.S. Department of Homeland Security (DHS) to conduct background checks on pending travelers.

**Growing Complexity**

Counterfeit visas are not as large a problem as they were 20 years ago. Advances in technology have made it very difficult for all but the most high-end document vendors to counterfeit them, and it is often cheaper and easier to obtain an authentic visa by malfeasance — bribing a consular officer — than it is to acquire a machine-readable counterfeit visa that will work. Obtaining a genuine U.S. passport or one from a visa-waiver country by using fraudulent breeder
documents (driver’s licenses and birth certificates, as Ahmed Ressam did) is also cheaper and easier. But in the case of non-visa waiver countries, this shift to the use of genuine identities and identity documents now highlights the need to secure the visa issuance process from fraud and malfeasance.

This shift to genuine-identity documents also means that most visa fraud cases involving potential terrorist operatives are going to be very complex. Rather than relying on obvious flags like false identities, the visa team consisting of clerks, consular officers, visa-fraud coordinators and Diplomatic Security Service (DSS) special agents needs to examine carefully not just the applicant’s identity but also his or her story in an attempt to determine if it is legitimate, and if there are any subtle indicators that the applicant has ties to radical groups (like people who lose their passports to disguise travel to places like Pakistan and Yemen). As in many other security programs, however, demeanor is also critically important, and a good investigator can often spot signs of deception during a visa interview (if one is conducted).

If the applicant’s documents and story check out, and there are no indicators of radical connections, it is very difficult to determine that an applicant is up to no good unless the U.S. government possesses some sort of intelligence indicating that the person may be involved in such activity. In terms of intelligence, there are a number of different databases, such as the Consular Lookout and Support System (CLASS), the main State Department database and the terrorism-specific Terrorist Identities Datamart Environment (TIDE) system. The databases are checked in order to determine if there is any derogatory information that would preclude a suspect from receiving a visa. These databases allow a number of U.S. government agencies to provide input — CLASS is tied into the Interagency Border Inspection System (IBIS) — and they allow these other agencies to have a stake in the visa issuance process. (It must be noted that, like any database, foreign language issues — such as the many ways to transliterate the name Mohammed into English — can often complicate the accuracy of visa lookout database entries and checks.)
Today the lookout databases are a far cry from what they were even 15 years ago, when many of the lists were contained on microfiche and checking them was laborious. During the microfiche era, mistakes were easily made, and some officers skipped the step of running the time-consuming name checks on people who did not appear to be potential terrorists. This is what happened in the case of a poor old blind imam who showed up at the U.S. Embassy in Khartoum in 1990 — and who turned out to be terrorist leader Sheikh Omar Ali Ahmed Abdul-Rahman. As an aside, although Rahman, known as the Blind Sheikh, did receive a U.S. visa, DSS special agents who investigated his case were able to document that he made material false statements on his visa application (such as claiming he had never been arrested) and were therefore able to build a visa fraud case against the Sheikh. The case never proceeded to trial, since the Sheikh was convicted on seditious conspiracy charges and sentenced to life in prison.

The U.S. government’s visa fraud investigation specialists are the special agents assigned to the U.S. Department of State’s DSS. In much the same way that U.S. Secret Service special agents work to ensure the integrity of the U.S. currency system through investigations of counterfeiting, DSS agents work to ensure the inviolability of U.S. passports and visas by investigating passport and visa fraud. The DSS has long assigned special agents to high fraud-threat countries like Nigeria to investigate passport and visa fraud in conjunction with the post’s consular affairs officers. In the Intelligence Reform and Terrorism Prevention Act of 2004, Congress ordered the State Department to establish a visa and passport security program. In response to this legislation, a memorandum of understanding was signed between the Bureau of Consular Affairs and the DSS to establish the Overseas Criminal Investigations Branch (OCI). The purpose of the OCI was to conduct investigations related to illegal passport and visa issuances or use and other investigations at U.S. embassies overseas. A special agent assigned to these duties at an overseas post is referred to as an investigative Assistant Regional Security Officer (or ARSO-I).
While the OCI and the ARSO-I program seemed promising at first, circumstance and bureaucratic hurdles have prevented the program from running to the best of its ability and meeting the expectations of the U.S. Congress.

Bureaucratic Shenanigans

As we’ve previously noted, there is a powerful element within the State Department that is averse to security and does its best to thwart security programs. DSS special agents refer to these people as Black Dragons. Even when Congress provides clear guidance to the State Department regarding issues of security (e.g., the Omnibus Diplomatic Security and Antiterrorism Act of 1986), the Black Dragons do their best to strangle the programs, and this constant struggle produces discernable boom-and-bust cycles, as Congress provides money for new security programs and the Black Dragons, who consider security counterproductive for diplomacy and armed State Department special agents undiplomatic, use their bureaucratic power to cut off those programs.

Compounding this perennial battle over security funding has been the incredible increase in protective responsibilities that the DSS has had to shoulder since 9/11. The bureau has had to provide a large number of agents to protect U.S. diplomats in places like Afghanistan and Pakistan and even staffed and supervised the protective detail for Afghan President Hamid Karzai for a few years. Two DSS special agents were also killed while protecting the huge number of U.S. diplomats assigned to reconstruction efforts in Iraq. One agent was killed in a rocket attack on the U.S. Embassy in Baghdad and the other by a suicide car-bomb attack in Mosul.

The demands of protection and bureaucratic strangulation by the Black Dragons, who have not embraced the concept of the ARSO-I program, has resulted in the OCI program being deployed very slowly. This means that of the 200 positions envisioned and internally programmed by Bureau of Consular Affairs and DSS in 2004, only 50 ARSO-I agents have been assigned to posts abroad as of this writing,
and a total of 123 ARSO-I agents are supposed to be deployed by the end of 2011. The other 77 ARSO-I positions were taken away from the OCI program by the department and used to provide more secretarial positions.

In the wake of State Department heel-dragging, other agencies are now seeking to fill the void.

**The Vultures Are Circling**

In a Feb. 9, 2010, editorial on GovernmentExecutive.com, former DHS Under Secretary for Border and Transportation Security Asa Hutchinson made a pitch for the DHS to become more involved in the visa-security process overseas, and he is pushing for funding more DHS positions at U.S. embassies abroad. To support his case that more DHS officers are needed for visa security, Hutchinson used the case of Umar Farouk Abdulmutallab as an example of why DHS needed a larger presence overseas.

Unfortunately, the Abdulmutallab case had nothing to do with visa fraud, and the presence of a DHS officer at post would certainly not have prevented him from receiving his initial visa. Abdulmutallab was first issued a U.S. visa in 2004, before he was radicalized during his university studies in the United Kingdom from 2005 to 2008, and he qualified for that visa according to the guidelines established by the U.S. government without fraud or deception. Of course, the fact that he came from a prominent Nigerian family certainly helped.

The problem in the Abdulmutallab case began when the CIA handled the interview of Abdulmutallab’s father when he walked into the embassy in November 2009 to report that his son had become
radicalized and that he feared his son was preparing for a suicide mission. The CIA did not share the information gleaned from that interview in a terrorism report cable (TERREP), or with the regional security officer at post or the ARSO-I. (The fact that the CIA, FBI and other agencies have assumed control over the walk-in program in recent years is also a serious problem, but that is a matter to be addressed separately.) Due to that lack of information-sharing, Abdulmutallab’s visa was not canceled as it could have and should have been. His name was also not added to the U.S. government’s no-fly list.

Again, had there been a DHS officer assigned to the embassy, he would not have been able to do any more than the ARSO-I already assigned to post, since he also would not have received the information from the CIA that would have indicated that Abdulmutallab’s visa needed to be revoked.

Once again, information was not shared in a counterterrorism case — a recurring theme in recent years. And once again the lack of information would have proved deadly had Abdulmutallab’s device not malfunctioned. Unfortunately, information-sharing is never facilitated by the addition of layers of bureaucracy. This is the reason why the addition of the huge new bureaucracy called the Office of the Director of National Intelligence has not solved the issue of information-sharing among intelligence agencies.

Hutchinson is correct when he notes that the DHS must go back to basics, but DHS has numerous other domestic programs that it must master the basics of — things like securing the border, overseeing port and cargo security, interior immigration and customs enforcement and ensuring airline security — before it should even consider expanding its presence overseas.

Adding another layer of DHS involvement in overseeing visa issuance and investigating visa fraud at diplomatic posts abroad is simply not going to assist in the flow of information in visa cases, whether criminal or terrorist in nature. Having another U.S. law enforcement agency interfacing with the host country police and security agencies regarding visa matters will also serve to cause confusion and
hamper efficient information flow. The problem illustrated by the Abdulmutallab case is not that the U.S. government lacks enough agencies operating in overseas posts; the problem is that the myriad agencies already there simply need to return to doing basic things like talking to each other. Getting the ARSO-I program funded and back on track is a basic step necessary to help in securing the visa process, but even that will not be totally effective unless the agencies at post do a better job of basic tasks like coordination and communication.

A Primer on Situational Awareness

June 10, 2010

The world is a wonderful place, but it can also be a dangerous one. In almost every corner of the globe militants of some political persuasion are plotting terror attacks — and these attacks can happen in London or New York, not just in Peshawar or Baghdad. Meanwhile, criminals operate wherever there are people, seeking to steal, rape, kidnap or kill.

Regardless of the threat, it is very important to recognize that criminal and terrorist attacks do not materialize out of thin air. In fact, quite the opposite is true. Criminals and terrorists follow a process when planning their actions, and this process has several distinct steps. This process has traditionally been referred to as the “terrorist attack cycle,” but if one looks at the issue thoughtfully, it becomes apparent that the same steps apply to nearly all crimes. Of course, there will be more time between steps in a complex crime like a kidnapping or car bombing than there will be between steps in a simple crime such as purse-snatching or shoplifting, where the steps can be completed quite rapidly. Nevertheless, the same steps are usually followed.

People who practice situational awareness can often spot this planning process as it unfolds and then take appropriate steps to avoid the dangerous situation or prevent it from happening altogether. Because
of this, situational awareness is one of the key building blocks of effective personal security — and when exercised by large numbers of people, it can also be an important facet of national security. Since situational awareness is so important, and because we discuss situational awareness so frequently in our analyses, we thought it would be helpful to discuss the subject in detail and provide a primer that can be used by people in all sorts of situations.

**Foundations**

First and foremost, it needs to be noted that being aware of one’s surroundings and identifying potential threats and dangerous situations is more of a mindset than a hard skill. Because of this, situational awareness is not something that can be practiced only by highly trained government agents or specialized corporate security countersurveillance teams. Indeed, it can be exercised by anyone with the will and the discipline to do so.

An important element of the proper mindset is to first recognize that threats exist. Ignorance or denial of a threat — or completely tuning out one’s surroundings while in a public place — makes a person’s chances of quickly recognizing the threat and avoiding it slim to none. This is why apathy, denial and complacency can be (and often are) deadly. A second important element is understanding the need to take responsibility for one’s own security. The resources of any government are finite and the authorities simply cannot be everywhere and cannot stop every criminal action. The same principle applies to private security at businesses or other institutions, like places of worship. Therefore, people need to look out for themselves and their neighbors.

Another important facet of this mindset is learning to trust your “gut” or intuition. Many times a person’s subconscious can notice subtle signs of danger that the conscious mind has difficulty quantifying or articulating. Many people who are victimized frequently experience such feelings of danger prior to an incident, but choose to ignore them. Even a potentially threatening person not making an
immediate move — or even if the person wanders off quickly after a moment of eye contact — does not mean there was no threat.

Levels of Awareness

People typically operate on five distinct levels of awareness. There are many ways to describe these levels (“Cooper’s colors,” for example, which is a system frequently used in law enforcement and military training), but perhaps the most effective way to illustrate the differences between the levels is to compare them to the different degrees of attention we practice while driving. For our purposes here we will refer to the five levels as “tuned out;” “relaxed awareness;” “focused awareness;” “high alert” and “comatose.”

The first level, tuned out, is like when you are driving in a very familiar environment or are engrossed in thought, a daydream, a song on the radio or even by the kids fighting in the backseat. Increasingly, cell phone calls and texting are also causing people to tune out while they drive. Have you ever gotten into the car and arrived somewhere without even really thinking about your drive there? If so, then you’ve experienced being tuned out.

The second level of awareness, relaxed awareness, is like defensive driving. This is a state in which you are relaxed but you are also watching the other cars on the road and are looking well ahead for potential road hazards. If another driver looks like he may not stop at the intersection ahead, you tap your brakes to slow your car in case he does not. Defensive driving does not make you weary, and you can drive this way for a long time if you have the discipline to keep yourself at this level, but it is very easy to slip into tuned-out mode. If you are practicing defensive driving you can still enjoy the trip, look at the scenery and listen to the radio, but you cannot allow yourself to get so engrossed in those distractions that they exclude everything else. You are relaxed and enjoying your drive, but you are still watching for road hazards, maintaining a safe following distance and keeping an eye on the behavior of the drivers around you.
The next level of awareness, focused awareness, is like driving in hazardous road conditions. You need to practice this level of awareness when you are driving on icy or slushy roads — or the roads infested with potholes and erratic drivers that exist in many third-world countries. When you are driving in such an environment, you need to keep two hands on the wheel at all times and have your attention totally focused on the road and the other drivers. You don’t dare take your eyes off the road or let your attention wander. There is no time for cell phone calls or other distractions. The level of concentration required for this type of driving makes it extremely tiring and stressful. A drive that you normally would not think twice about will totally exhaust you under these conditions because it demands your prolonged and total concentration.

The fourth level of awareness is high alert. This is the level that induces an adrenaline rush, a prayer and a gasp for air all at the same time — “Watch out! There’s a deer in the road! Hit the brakes!” This also happens when that car you are watching doesn’t stop at the stop sign and pulls out right in front of you. High alert can be scary, but at this level you are still able to function. You can hit your brakes and keep your car under control. In fact, the adrenalin rush you get at this stage can sometimes even aid your reflexes. But, the human body can tolerate only short periods of high alert before becoming physically and mentally exhausted.

The last level of awareness, comatose, is what happens when you literally freeze at the wheel and cannot respond to stimuli, either because you have fallen asleep, or, at the other end of the spectrum, because you are petrified from panic. It is this panic-induced paralysis that concerns us most in relation to situational awareness. The comatose level of awareness (or perhaps more accurately, lack of awareness) is where you go into shock, your brain ceases to process information and you simply cannot react to the reality of the situation. Many times when this happens, a person can go into denial, believing that “this can’t be happening to me,” or the person can feel as though he or she is observing, rather than actually participating in, the event. Often, the passage of time will seem to grind to a halt. Crime victims
frequently report experiencing this sensation and being unable to act during an unfolding crime.

Finding the Right Level

Now that we’ve discussed the different levels of awareness, let’s focus on identifying what level is ideal at a given time. The body and mind both require rest, so we have to spend several hours each day at the comatose level while asleep. When we are sitting at our homes watching a movie or reading a book, it is perfectly fine to operate in the tuned-out mode. However, some people will attempt to maintain the tuned-out mode in decidedly inappropriate environments (e.g., when they are out on the street at night in a third-world barrio), or they will maintain a mindset wherein they deny that they can be victimized by criminals. “That couldn’t happen to me, so there’s no need to watch for it.” They are tuned out.

Some people are so tuned out as they go through life that they miss even blatant signs of pending criminal activity directed specifically at them. In 1992, an American executive living in the Philippines was kidnapped by a Marxist kidnapping gang in Manila known as the “Red Scorpion Group.” When the man was debriefed following his rescue, he described in detail how the kidnappers had blocked off his car in traffic and abducted him. Then, to the surprise of the debriefing team, he said that on the day before he was abducted, the same group of guys had attempted to kidnap him at the exact same location, at the very same time of day and driving the same vehicle. The attackers had failed to adequately box his car in, however, and his driver was able to pull around the blocking vehicle and proceed to the office.

Since the executive did not consider himself to be a kidnapping target, he had just assumed that the incident the day before his abduction was “just another close call in crazy Manila traffic.” The executive and his driver had both been tuned out. Unfortunately, the executive paid for this lack of situational awareness by having to withstand an extremely traumatic kidnapping, which included almost being killed
in the dramatic Philippine National Police operation that rescued him.

If you are tuned out while you are driving and something happens — say, a child runs out into the road or a car stops quickly in front of you — you will not see the problem coming. This usually means that you either do not see the hazard in time to avoid it and you hit it, or you totally panic and cannot react to it — neither is good. These reactions (or lack of reaction) occur because it is very difficult to change mental states quickly, especially when the adjustment requires moving several steps, say, from tuned out to high alert. It is like trying to shift your car directly from first gear into fifth and it shudders and stalls. Many times, when people are forced to make this mental jump and they panic (and stall), they go into shock and will actually freeze and be unable to take any action — they go comatose. This happens not only when driving but also when a criminal catches someone totally unaware and unprepared. While training does help people move up and down the alertness continuum, it is difficult for even highly trained individuals to transition from tuned out to high alert. This is why police officers, federal agents and military personnel receive so much training on situational awareness.

It is critical to stress here that situational awareness does not mean being paranoid or obsessively concerned about your security. It does not mean living with the irrational expectation that there is a dangerous criminal lurking behind every bush. In fact, people simply cannot operate in a state of focused awareness for extended periods, and high alert can be maintained only for very brief periods before exhaustion sets in. The “flight or fight” response can be very helpful if it can be controlled. When it gets out of control, however, a constant stream of adrenaline and stress is simply not healthy for the body or the mind. When people are constantly paranoid, they become mentally and physically burned out. Not only is this dangerous to physical and mental health, but security also suffers because it is very hard to be aware of your surroundings when you are a complete basket case. Therefore, operating constantly in a state of high alert is not the answer, nor is operating for prolonged periods in a state of focused
alert, which can also be overly demanding and completely enervating. This is the process that results in alert fatigue. The human body was simply not designed to operate under constant stress. People (even highly skilled operators) require time to rest and recover.

Because of this, the basic level of situational awareness that should be practiced most of the time is relaxed awareness, a state of mind that can be maintained indefinitely without all the stress and fatigue associated with focused awareness or high alert. Relaxed awareness is not tiring, and it allows you to enjoy life while rewarding you with an effective level of personal security. When you are in an area where there is potential danger (which, by definition, is almost anywhere), you should go through most of your day in a state of relaxed awareness. Then if you spot something out of the ordinary that could be a potential threat, you can “dial yourself up” to a state of focused awareness and take a careful look at that potential threat (and also look for others in the area).

If the potential threat proves innocuous, or is simply a false alarm, you can dial yourself back down into relaxed awareness and continue on your merry way. If, on the other hand, you look and determine that the potential threat is a probable threat, seeing it in advance allows you to take actions to avoid it. You may never need to elevate to high alert, since you have avoided the problem at an early stage. However, once you are in a state of focused awareness you are far better prepared to handle the jump to high alert if the threat does change from potential to actual — if the three guys lurking on the corner do start coming toward you and look as if they are reaching for weapons. The chances of you going comatose are far less if you jump from focused awareness to high alert than if you are caught by surprise and “forced” to go into high alert from tuned out. An illustration of this would be the difference between a car making a sudden stop in front of a person when the driver is practicing defensive driving, compared to a car that makes a sudden stop in front of a person when the driver is sending a text message.

Of course, if you know that you must go into an area that is very dangerous, you should dial yourself up to focused awareness when
you are in that area. For example, if there is a specific section of highway where a lot of improvised explosive devices detonate and ambushes occur, or if there is a part of a city that is controlled (and patrolled) by criminal gangs — and you cannot avoid these danger areas for whatever reason — it would be prudent to heighten your level of awareness when you are in those areas. An increased level of awareness is also prudent when engaging in common or everyday tasks, such as visiting an ATM or walking to the car in a dark parking lot. The seemingly trivial nature of these common tasks can make it all too easy to go on “autopilot” and thus expose yourself to threats. When the time of potential danger has passed, you can then go back to a state of relaxed awareness.

This process also demonstrates the importance of being familiar with your environment and the dangers that are present there. Such awareness allows you to avoid many threats and to be on the alert when you must venture into a dangerous area.

Clearly, few of us are living in the type of intense threat environment currently found in places like Mogadishu, Juarez or Kandahar. Nonetheless, average citizens all over the world face many different kinds of threats on a daily basis — from common thieves and assailants to criminals and mentally disturbed individuals aiming to conduct violent acts to militants wanting to carry out large-scale attacks against subways and aircraft.

Many of the steps required to conduct these attacks must be accomplished in a manner that makes the actions visible to the potential victim and outside observers. It is at these junctures that people practicing situational awareness can detect these attack steps, avoid the danger and alert the authorities. When people practice situational awareness they not only can keep themselves safer but they can also help keep others safe. And when groups of people practice situational awareness together they can help keep their schools, houses of worship, workplaces and cities safe from danger.

And as we’ve discussed many times before, as the terrorist threat continues to devolve into one almost as diffuse as the criminal
A STRATFOR GUIDE TO SECURITY WHILE ABROAD

Terrorism, Vigilance and the Limits of the War on Terror

October 5, 2010

The U.S. government issued a warning Oct. 3 advising Americans traveling to Europe to be “vigilant.” U.S. intelligence apparently has acquired information indicating that al Qaeda is planning to carry out attacks in European cities similar to those carried out in Mumbai, India, in November 2008. In Mumbai, attackers armed with firearms, grenades and small, timed explosive devices targeted hotels frequented by Western tourists and other buildings in an attack that took three days to put down.

European security forces are far better trained and prepared than their Indian counterparts, and such an attack would be unlikely to last for hours, much less days, in a European country. Still, armed assaults conducted by suicide operatives could be expected to cause many casualties and certainly create a dramatic disruption to economic and social life.

The first question to ask about the Oct. 3 warning, which lacked specific and actionable intelligence, is how someone can be vigilant against such an attack. There are some specific steps that people can and should take to practice good situational awareness as well as some common-sense travel-security precautions. But if you find yourself sleeping in a hotel room as gunmen attack the building, rush to your floor and start entering rooms, a government warning simply to be vigilant would have very little meaning.

The world is awash in intelligence about terrorism. Most of it is meaningless speculation, a conversation intercepted between two Arabs about how they’d love to blow up London Bridge. The problem,
of course, is how to distinguish between idle chatter and actual attack planning. There is no science involved in this, but there are obvious guidelines. Are the people known to be associated with radical Islamists? Do they have the intent and capability to conduct such an attack? Were any specific details mentioned in the conversation that can be vetted? Is there other intelligence to support the plot discussed in the conversation?

The problem is that what appears quite obvious in the telling is much more ambiguous in reality. At any given point, the government could reasonably raise the alert level if it wished. That it doesn't raise it more frequently is tied to three things. First, the intelligence is frequently too ambiguous to act on. Second, raising the alert level warns people without really giving them any sense of what to do about it. Third, it can compromise the sources of its intelligence.

The current warning is a perfect example of the problem. We do not know what intelligence the U.S. government received that prompted the warning, and the public descriptions of the intelligence likely do not reveal everything that the government knows. We do know that a German citizen was arrested in Afghanistan in July and has allegedly provided information regarding this threat, but there are likely other sources contributing to the warning, since the U.S. government considered the intelligence sufficient to cause concern. The Obama administration leaked on Saturday that it might issue the warning, and indeed it did.

The government did not recommend that Americans not travel to Europe. That would have affected the economy and infuriated Europeans. Leaving tourism aside, since tourism season is largely over, a lot of business is transacted by Americans in Europe. The government simply suggested vigilance. Short of barring travel, there was nothing effective the government could do. So it shifted the burden to travelers. If no attack occurs, nothing is lost. If an attack occurs, the government can point to the warning and the advice. Those hurt or killed would not have been vigilant.

This is not to belittle the U.S. government on this. Having picked up the intelligence it can warn the public or not. The public has a
right to know, and the government is bound by law and executive order to provide threat information. But the reason that its advice is so vague is that there is no better advice to give. The government is not so much washing its hands of the situation as acknowledging that there is not much that anyone can do aside from the security measures travelers should already be practicing.

The alert serves another purpose beyond alerting the public. It communicates to the attackers that their attack has been detected if not penetrated, and that the risks of the attack have pyramided. Since these are most likely suicide attackers not expecting to live through the attack, the danger is not in death. It is that the Americans or the Europeans might have sufficient intelligence available to thwart the attack. From the terrorist point of view, losing attackers to death or capture while failing to inflict damage is the worst of all possible scenarios. Trained operatives are scarce, and like any strategic weapon they must be husbanded and, when used, cause maximum damage. When the attackers do not know what Western intelligence knows, their risk of failure is increased along with the incentive to cancel the attack. A government warning, therefore, can prevent an attack.

In addition, a public warning can set off a hunt for the leak within al Qaeda. Communications might be shut down while the weakness is examined. Members of the organization might be brought under suspicion. The warning can generate intense uncertainty within al Qaeda as to how much Western intelligence knows. The warning, if it correlates with an active plot, indicates a breach of security, and a breach of security can lead to a witch-hunt that can paralyze an organization.

Therefore, the warning might well have served a purpose, but the purpose was not necessarily to empower citizens to protect themselves from terrorists. Indeed, there might have been two purposes. One might have been to disrupt the attack and the attackers. The other might have been to cover the government if an attack came.

In either case, it has to be recognized that this sort of warning breeds cynicism among the public. If the warning is intended to empower citizens, it engenders a sense of helplessness, and if no
attack occurs, it can also lead to alert fatigue. What the government is saying to its citizenry is that, in the end, it cannot guarantee that there won't be an attack and therefore its citizens are on their own. The problem with that statement is not that the government isn't doing its job but that the job cannot be done. The government can reduce the threat of terrorism. It cannot eliminate it.

This brings us to the strategic point. The defeat of jihadist terror cells cannot be accomplished defensively. Homeland security can mitigate the threat, but it can never eliminate it. The only way to eliminate it is to destroy all jihadist cells and prevent the formation of new cells by other movements or by individuals forming new movements, and this requires not just destroying existing organizations but also the radical ideology that underlies them. To achieve this, the United States and its allies would have to completely penetrate a population of about 1.3 billion people and detect every meeting of four or five people planning to create a terrorist cell. And this impossible task would not even address the problem of lone-wolf terrorists. It is simply impossible to completely dominate and police the entire world, and any effort to do so would undoubtedly induce even more people to turn to terrorism in opposition to the global police state.

Will Rogers was asked what he might do to deal with the German U-boat threat in World War I. He said he would boil away the Atlantic, revealing the location of the U-boats that could then be destroyed. Asked how he would do this, he answered that that was a technical question and he was a policymaker.

The idea of suppressing jihadist terrorism through direct military action in the Islamic world would be an idea Will Rogers would have appreciated. It is a superb plan from a policymaking perspective. It suffers only from the problem of technical implementation. Even native Muslim governments motivated to suppress Islamic terrorism, like those in Egypt, Saudi Arabia, Algeria or Yemen, can't achieve this goal absolutely. The idea that American troops, outnumbered and not speaking the language or understanding the culture, can do this is simply not grounded in reality.
The United States and Europe are going to be attacked by jihadist terrorists from time to time, and innocent people are going to be killed, perhaps in the thousands again. The United States and its allies can minimize the threat through covert actions and strong defenses, but they cannot eliminate it. The hapless warning to be vigilant that was issued this past weekend is the implicit admission of this fact.

This is not a failure of will or governance. The United States can’t conceivably mount the force needed to occupy the Islamic world, let alone pacify it to the point where it can’t be a base for terrorists. Given that the United States can’t do this in Afghanistan, the idea that it might spread this war throughout the Islamic world is unsupportable.

The United States and Europe are therefore dealing with a threat that cannot be stopped by their actions. The only conceivably effective actions would be those taken by Muslim governments, and even those are unlikely to be effective. There is a deeply embedded element within a small segment of the Islamic world that is prepared to conduct terror attacks, and this element will occasionally be successful.

All people hate to feel helpless, and this trait is particularly strong among Americans. There is a belief that America can do anything and that something can and should be done to eliminate terrorism and not just mitigate it. Some Americans believe sufficiently ruthless military action can do it. Others believe that reaching out in friendship might do it. In the end, the terrorist element will not be moved by either approach, and no amount of vigilance (or new bureaucracies) will stop them.

It would follow then that the West will have to live with the terrorist threat for the foreseeable future. This does not mean that military, intelligence, diplomatic, law-enforcement or financial action should be stopped. Causing most terrorist attempts to end in failure is an obviously desirable end. It not only blocks the particular action but also discourages others. But the West will have to accept that there are no measures that will eliminate the threat entirely. The danger will persist.

Effort must be made to suppress it, but the level of effort has to be proportional not to the moral insult of the terrorist act but
to considerations of other interests beyond counterterrorism. The United States has an interest in suppressing terrorism. Beyond a certain level of effort, it will reach a point of diminishing returns. Worse, by becoming narrowly focused on counterterrorism and over-committing resources to it, the United States will leave other situations unattended as it focuses excessively on a situation it cannot improve.

The request that Americans be vigilant in Europe represents the limits of power on the question of terrorism. There is nothing else that can be done and what can be done is being done. It also drives home the fact that the United States and the West in general cannot focus all of its power on solving a problem that is beyond its power to solve. The long war against terrorism will not be the only war fought in the coming years. The threat of jihadism must be put in perspective and the effort aligned with what is effective. The world is a dangerous place, as they say, and jihadism is only one of the dangers.

How to Respond to Terrorism Threats and Warnings

October 7, 2010

In “Terrorism, Vigilance and the Limits of the War on Terror,” we wrote that recent warnings by the U.S. government of possible terrorist attacks in Europe illustrate the fact that jihadist terrorism is a threat the world will have to live with for the foreseeable future. Certainly, every effort should be made to disrupt terrorist groups and independent cells, or lone wolves, and to prevent attacks. In practical terms, however, it is impossible to destroy the phenomenon of terrorism. At this very moment, jihadists in various parts of the world are seeking ways to carry out attacks against targets in the United States and Europe and, inevitably, some of these plots will succeed. George also noted that, all too often, governments raise the alert level regarding a potential terrorist attack without giving the public
any actionable intelligence, which leaves people without any sense of what to do about the threat.

The world is a dangerous place, and violence and threats of violence have always been a part of the human condition. Hadrian’s Wall was built for a reason, and there is a reason we all have to take our shoes off at the airport today. While there is danger in the world, that does not mean people have to hide under their beds and wait for something tragic to happen. Nor should people count on the government to save them from every potential threat. Even very effective military, counterterrorism, law enforcement and homeland security efforts (and their synthesis — no small challenge itself) cannot succeed in eliminating the threat because the universe of potential actors is simply too large and dispersed. There are, however, common-sense security measures that people should take regardless of the threat level.

Situational Awareness

The foundation upon which all personal security measures are built is situational awareness. Before any measures can be taken, one must first recognize that threats exist. Ignorance or denial of a threat and paying no attention to one’s surroundings make a person’s chances of quickly recognizing a threat and then reacting in time to avoid it quite remote. Only pure luck or the attacker’s incompetence can save such a person. Apathy, denial and complacency, therefore, can be (and often are) deadly. A second important element is recognizing the need to take responsibility for one’s own security. The resources of any government are finite and the authorities simply cannot be everywhere and stop every terrorist act.

As we’ve mentioned previously, terrorist attacks do not magically materialize. They are part of a deliberate process consisting of several distinct steps. And there are many points in that process where the plotters are vulnerable to detection. People practicing situational awareness can often spot this planning process as it unfolds and take appropriate steps to avoid the dangerous situation or prevent it from
happening altogether. But situational awareness can transcend the individual. When it is exercised by a large number of people, situational awareness can also be an important facet of national security. The citizens of a nation have far more capability to notice suspicious behavior than the intelligence services and police, and this type of grassroots defense is growing more important as the terrorist threat becomes increasingly diffuse and as attackers focus more and more on soft targets. This is something we noted in last week’s Security Weekly when we discussed the motives behind warnings issued by the chief of France’s Central Directorate of Interior Intelligence regarding the terrorist threat France faces.

It is important to emphasize that practicing situational awareness does not mean living in a state of constant fear and paranoia. Fear and paranoia are in fact counterproductive to good personal security. Now, there are times when it is prudent to be in a heightened state of awareness, but people are simply not designed to operate in that state for prolonged periods. Rather, situational awareness is best practiced in what we refer to as a state of relaxed awareness. Relaxed awareness allows one to move into a higher state of alert as the situation requires, a transition that is very difficult if one is not paying any attention at all. This state of awareness permits people to go through life attentively, but in a relaxed, sustainable and less-stressful manner. (A detailed primer on how to effectively exercise situational awareness can be found here.)

**Preparedness**

In the immediate wake of a terrorist attack or some other disaster, disorder and confusion are often widespread as a number of things happen simultaneously. Frequently, panic erupts as people attempt to flee the immediate scene of the attack. At the same time, police, fire and emergency medical units all attempt to respond to the scene, so there can be terrible traffic and pedestrian crowd-control problems. This effect can be magnified by smoke and fire, which can impair vision, affect breathing and increase the sense of panic. Indeed,
frequently many of the injuries produced by terrorist bombings are not a direct result of the blast or even shrapnel but are caused by smoke inhalation and trampling.

In many instances, an attack will damage electrical lines or electricity will be cut off as a precautionary measure. Elevators also can be reserved for firefighters. This means people are frequently trapped in subway tunnels or high-rises and might be forced to escape through smoke-filled tunnels or stairwells. Depending on the incident, bridges, tunnels, subway lines and airports can be closed, or merely jammed to a standstill. For those driving, this gridlock could be exacerbated if the power is out to traffic signals.

In the midst of the confusion and panic, telephone and cell phone usage will soar. Even if the main trunk lines and cell towers have not been damaged by the attack or taken down by the loss of electricity, a huge spike in activity will quickly overload the exchanges and cell networks. This causes ripples of chaos and disruption to roll outward from the scene as people outside the immediate vicinity of the attack zone hear about the incident and wonder what has become of loved ones who were near the attack site.

Those caught in the vicinity of an attack have the best chance of escaping and reconnecting with loved ones if they have a personal contingency plan. Such plans should be in place for each regular location — home, work and school — that each member of the family frequents and should cover what that person will do and where he or she will go should an evacuation be necessary. Obviously, parents of younger children need to coordinate more closely with their children’s schools than parents of older children. Contingency plans need to establish meeting points for family members who might be split up — and backup points in case the first or second point is also affected by the disaster.

The lack of ability to communicate with loved ones because of circuit overload or other phone-service problems can greatly enhance the sense of panic during a crisis. Perhaps the most value derived from having personal and family contingency plans is a reduction in the stress that results from not being able to immediately contact a loved
one. Knowing that everyone is following the plan frees each person to concentrate on the more pressing issue of evacuation. Additionally, someone who waits until he or she has contacted all loved ones before evacuating might not make it out. Contingency planning should also include a communication plan that provides alternate means of communication in case the telephone networks go down.

People who work or live in high-rises, frequently travel or take subways should consider purchasing and carrying a couple of pieces of equipment that can greatly assist their ability to evacuate such locations. One of these is a smoke hood, a protective device that fits over the head and provides protection from smoke inhalation. The second piece of equipment is a flashlight small enough to fit in a pocket, purse or briefcase. Such a light could prove invaluable in a crisis situation at night or when the power goes out in a large building or subway. Some of the small aluminum flashlights also double as a handy self-defense weapon.

It is also prudent to maintain a small “fly-away” kit containing clothes, water, a first aid kit, nutritional bars, medications and toiletry items for you and your family in your home or office. Items such as a battery- or hand-powered radio, a multitool knife and duct tape can also prove quite handy in an emergency. The kit should be kept in convenient place, ready to grab on the way out.

Contingency planning is important because, when confronted with a dire emergency, many people simply do not know what to do. Not having determined their options in advance — and in shock over the events of the day — they are unable to think clearly enough to establish a logical plan and instead wander aimlessly around, or simply freeze in panic.

The problems are magnified when there are large numbers of people caught unprepared, trying to find solutions, and scrambling for the same emergency materials you are. Having an established plan in place gives even a person who is in shock or denial and unable to think clearly a framework to lean on and a path to follow. It also allows them to get a step ahead of everybody else and make positive
progress toward more advanced stages of self-protection or evacuation rather than milling around among the dazed and confused.

**Travel Security**

Of course, not all emergencies occur close to home, and the current U.S. government warning was issued for citizens traveling in Europe, so a discussion here of travel security is certainly worthwhile. Obviously, the need to practice situational awareness applies during travel as much as it does anywhere else. There are, however, other small steps that can be taken to help keep one safe from criminals and terrorists when away from home.

In recent years, terrorists have frequently targeted hotels, which became attractive soft targets when embassies and other diplomatic missions began hardening their security. This means that travelers should not only look at the cost of a hotel room but also carefully consider the level of security provided by a hotel before they make a choice. In past attacks, such as the November 2005 hotel bombings in Amman, Jordan, the attackers surveilled a number of facilities and selected those they felt were the most vulnerable. Location is also a critical consideration. Hotels that are close to significant landmarks or hotels that are themselves landmarks should be considered carefully.

Travelers should also request rooms that are somewhere above the ground floor to prevent a potential attacker from easily entering the room but not more than several stories up so that a fire department extension ladder can reach them in an emergency. Rooms near the front of the hotel or facing the street should be avoided when possible; attacks against hotels typically target the foyer or lobby at the front of the building. Hotel guests should also learn where the emergency exits are and physically walk the route to ensure it is free from obstruction. It is not unusual to find emergency exits blocked or chained and locked in Third World countries. And it is prudent to avoid lingering in high-risk areas such as hotel lobbies, the front desk and entrance areas and bars. Western diplomats, business people
and journalists who frequently congregate in these areas have been attacked or otherwise targeted on numerous occasions in many different parts of the world.

There are also a number of practical steps that can be taken to stay safe at foreign airports, aboard public transportation and while on aircraft.

**Perspective**

Finally, it is important to keep the terrorist threat in perspective. As noted above, threats of violence have always existed, and the threat posed to Europe by jihadist terrorists today is not much different from that posed by Marxist or Palestinian terrorists in the 1970s. It is also far less of a threat than the people of Europe experienced from the army of the Umayyad Caliphate at Tours in 732, or when the Ottoman Empire attacked Vienna in 1683. Indeed, far more people (including tourists) will be affected by crime than terrorism in Europe this year, and more people will be killed in European car accidents than terrorist attacks.

If people live their lives in a constant state of fear, those who seek to terrorize them have won. Terror attacks are a tactic used by a variety of militant groups for a variety of ends. As the name implies, terrorism is intended to produce a psychological impact that far outweighs the actual physical damage caused by the attack itself. Denying would-be terrorists this multiplication effect, as the British largely did after the July 2005 subway bombings, prevents them from accomplishing their greater goals. Terror can be countered when people assume the proper mindset and then take basic security measures and practice relaxed awareness. These elements work together to dispel paranoia and to prevent the fear of terrorism from robbing people of the joy of life.
Aviation Security Threats and Realities
November 23, 2010

Over the past few weeks, aviation security — specifically, enhanced passenger-screening procedures — has become a big issue in the media. The discussion of the topic has become even more fervent as we enter Thanksgiving weekend, which is historically one of the busiest travel periods of the year. As this discussion has progressed, we have been asked repeatedly by readers and members of the press for our opinion on the matter.

We have answered such requests from readers, and we have done a number of media interviews, but we’ve resisted writing a fresh analysis on aviation security because, as an organization, our objective is to lead the media rather than follow the media regarding a particular topic. We want our readers to be aware of things before they become pressing public issues, and when it comes to aviation-security threats and the issues involved with passenger screening, we believe we have accomplished this. Many of the things now being discussed in the media are things we’ve written about for years.

When we were discussing this topic internally and debating whether to write about it, we decided that since we have added so many new readers over the past few years, it might be of interest to our expanding readership to put together an analysis that reviews the material we’ve published and that helps to place the current discussion into the proper context. We hope our longtime readers will excuse the repetition.

We believe that this review will help establish that there is a legitimate threat to aviation, that there are significant challenges in trying to secure aircraft from every conceivable threat, and that the response of aviation security authorities to threats has often been slow and reactive rather than thoughtful and proactive.

Threats
Commercial aviation has been threatened by terrorism for decades now. From the first hijackings and bombings in the late 1960s to last
month’s attempt against the UPS and FedEx cargo aircraft, the threat has remained constant. As we have discussed for many years, jihadists have long had a fixation with attacking aircraft. When security measures were put in place to protect against Bojinka-style attacks in the 1990s — attacks that involved modular explosive devices smuggled onto planes and left aboard — the jihadists adapted and conducted 9/11-style attacks. When security measures were put in place to counter 9/11-style attacks, the jihadists quickly responded by going to onboard suicide attacks with explosive devices concealed in shoes. When that tactic was discovered and shoes began to be screened, they switched to devices containing camouflaged liquid explosives. When that plot failed and security measures were altered to restrict the quantity of liquids that people could take aboard aircraft, we saw the jihadists alter the paradigm once more and attempt the underwear-bomb attack last Christmas.

In a special edition of Inspire magazine released last weekend, al Qaeda in the Arabian Peninsula (AQAP) noted that, due to the increased passenger screening implemented after the Christmas Day 2009 attempt, the group’s operational planners decided to employ explosive devices sent via air cargo (we have written specifically about the vulnerability of air cargo to terrorist attacks).

Finally, it is also important to understand that the threat does not emanate just from jihadists like al Qaeda and its regional franchises. Over the past several decades, aircraft have been attacked by a number of different actors, including North Korean intelligence officers, Sikh, Palestinian and Hezbollah militants and mentally disturbed individuals like the Unabomber, among others.

Realities

While understanding that the threat is very real, it is also critical to recognize that there is no such thing as absolute, foolproof security. This applies to ground-based facilities as well as aircraft. If security procedures and checks have not been able to keep contraband out of high-security prisons, it is unreasonable to expect them to be able
to keep unauthorized items off aircraft, where (thankfully) security checks of crew and passengers are far less invasive than they are for prisoners. As long as people, luggage and cargo are allowed aboard aircraft, and as long as people on the ground crew and the flight crew have access to aircraft, aircraft will remain vulnerable to a number of internal and external threats.

This reality is accented by the sheer number of passengers that must be screened and number of aircraft that must be secured. According to figures supplied by the Transportation Security Administration (TSA), in 2006, the last year for which numbers are available, the agency screened 708,400,522 passengers on domestic flights and international flights coming into the United States. This averages out to over 1.9 million passengers per day.

Another reality is that, as mentioned above, jihadists and other people who seek to attack aircraft have proven to be quite resourceful and adaptive. They carefully study security measures, identify vulnerabilities and then seek to exploit them. Indeed, last September, when we analyzed the innovative designs of the explosive devices employed by AQAP, we called attention to the threat they posed to aviation more than three months before the Christmas 2009 bombing attempt. As we look at the issue again, it is not hard to see, as we pointed out then, how their innovative efforts to camouflage explosives in everyday items and hide them inside suicide operatives’ bodies will continue and how these efforts will be intended to exploit vulnerabilities in current screening systems.

As we wrote in September 2009, getting a completed explosive device or its components by security and onto an aircraft is a significant challenge, but it is possible for a resourceful bombmaker to devise ways to overcome that challenge. The latest issue of Inspire magazine demonstrated how AQAP has done some very detailed research to identify screening vulnerabilities. As the group noted in the magazine: “The British government said that if a toner weighs more than 500 grams it won’t be allowed on board a plane. Who is the genius who came up with this suggestion? Do you think that we have nothing to send but printers?”
AQAP also noted in the magazine that it is working to identify innocuous substances like toner ink that, when X-rayed, will appear similar to explosive compounds like PETN, since such innocuous substances will be ignored by screeners. With many countries now banning cargo from Yemen, it will be harder to send those other items in cargo from Sanaa, but the group has shown itself to be flexible, with the underwear-bomb operative beginning his trip to Detroit out of Nigeria rather than Yemen. In the special edition of Inspire, AQAP also specifically threatened to work with allies to launch future attacks from other locations.

Drug couriers have been transporting narcotics hidden inside their bodies aboard aircraft for decades, and prisoners frequently hide drugs, weapons and even cell phones inside body cavities. It is therefore only a matter of time before this same tactic is used to smuggle plastic explosives or even an entire non-metallic explosive device onto an aircraft — something that would allow an attacker to bypass metal detectors and backscatter X-ray inspection and pass through external pat-downs.

Look for the Bomber, Not Just the Bomb

This ability to camouflage explosives in a variety of different ways, or hide them inside the bodies of suicide operatives, means that the most significant weakness of any suicide-attack plan is the operative assigned to conduct the attack. Even in a plot to attack 10 or 12 aircraft, a group would need to manufacture only about 12 pounds of high explosives — about what is required for a single, small suicide device and far less than is required for a vehicle-borne improvised explosive device. Because of this, the operatives are more of a limiting factor than the explosives themselves; it is far more difficult to find and train 10 or 12 suicide bombers than it is to produce 10 or 12 devices.

A successful attack requires operatives who are not only dedicated enough to initiate a suicide device without getting cold feet; they must also possess the nerve to calmly proceed through airport security
checkpoints without alerting officers that they are up to something sinister. This set of tradecraft skills is referred to as demeanor, and while remaining calm under pressure and behaving normally may sound simple in theory, practicing good demeanor under the extreme pressure of a suicide operation is very difficult. Demeanor has proved to be the Achilles’ heel of several terror plots, and it is not something that militant groups have spent a great deal of time teaching their operatives. Because of this, it is frequently easier to spot demeanor mistakes than it is to find well-hidden explosives. Such demeanor mistakes can also be accentuated, or even induced, by contact with security personnel in the form of interviews, or even by unexpected changes in security protocols that alter the security environment a potential attacker is anticipating and has planned for.

There has been much discussion of profiling, but the difficulty of creating a reliable and accurate physical profile of a jihadist, and the adaptability and ingenuity of the jihadist planners, means that any attempt at profiling based only on race, ethnicity or religion is doomed to fail. In fact, profiling can prove counterproductive to good security by blinding people to real threats. They will dismiss potential malefactors who do not fit the specific profile they have been provided.

In an environment where the potential threat is hard to identify, it is doubly important to profile individuals based on their behavior rather than their ethnicity or nationality — what we refer to as focusing on the “how” instead of the “who.” Instead of relying on physical profiles, which allow attack planners to select operatives who do not match the profiles being selected for more intensive screening, security personnel should be encouraged to exercise their intelligence, intuition and common sense. A Caucasian U.S. citizen who shows up at the U.S. Embassy in Nairobi or Dhaka claiming to have lost his passport may be far more dangerous than some random Pakistani or Yemeni citizen, even though the American does not appear to fit the profile for requiring extra security checks.

However, when we begin to consider traits such as intelligence, intuition and common sense, one of the other realities that must
be faced with aviation security is that, quite simply, it is not an area where the airlines or governments have allocated the funding required to hire the best personnel. Airport screeners make far less than FBI special agents or CIA case officers and receive just a fraction of the training. Before 9/11, most airports in the United States relied on contract security guards to conduct screening duties. After 9/11, many of these same officers went from working for companies like Wackenhut to being TSA employees. There was no real effort made to increase the quality of screening personnel by offering much higher salaries to recruit a higher caliber of candidate.

There is frequent mention of the need to make U.S. airport security more like that employed in Israel. Aside from the constitutional and cultural factors that would prevent American airport screeners from ever treating Muslim travelers the way they are treated by El Al, another huge difference is simply the amount of money spent on salaries and training for screeners and other security personnel. El Al is also aided by the fact that it has a very small fleet of aircraft that fly only a small number of passengers to a handful of destinations.

Additionally, airport screening duty is simply not glamorous work. Officers are required to work long shifts conducting monotonous checks and are in near constant contact with a traveling public that can at times become quite surly when screeners follow policies established by bureaucrats at much higher pay grades. Granted, there are TSA officers who abuse their authority and do not exhibit good interpersonal skills, but anyone who travels regularly has also witnessed fellow travelers acting like idiots.

While it is impossible to keep all contraband off aircraft, efforts to improve technical methods and procedures to locate weapons and IED components must continue. However, these efforts must not only be reacting to past attacks and attempts but should also be looking forward to thwart future attacks that involve a shift in the terrorist paradigm. At the same time, the often-overlooked human elements of airport security, including situational awareness, observation and intuition, need to be emphasized now more than ever. It is
those soft skills that hold the real key to looking for the bomber and not just the bomb.

The Moscow Attack and Airport Security
January 27, 2011

The Jan. 24 bombing at Moscow’s Domodedovo International Airport killed 35 people and injured more than 160. The attack occurred at approximately 4:40 p.m. as passengers from several arriving international flights were leaving the airport after clearing immigration and customs. The attacker (or attackers; reports are still conflicting over whether the attack was conducted by a man or a man and a woman together) entered the international arrivals hall of the airport, a part of the facility that is outside the secure area and that is commonly packed with crowds of relatives and taxi and limo drivers waiting to meet travelers.

Once the attacker was in the midst of the waiting crowd and exiting passengers, the improvised explosive device that he (or she) carried was detonated. It is not clear at this point whether the device was command-detonated by the attacker as a traditional suicide bomb or if the device was remotely detonated by another person. The attack was most likely staged by Islamist militants from Russia’s Northern Caucasus region who have conducted a long series of attacks in Russia, including the Aug. 24, 2004, suicide bombings that destroyed two Russian airliners.

The Domodedovo attack serves as a striking illustration of several trends we have been following for years now, including the difficulty of preventing attacks against soft targets, the resourcefulness of militants in identifying such targets and the fixation militants have on aviation-related targets.
Soft Targets

By definition, soft targets are those targets that are vulnerable to attack due to the absence of adequate security. Adequate security may be absent for a number of reasons, including disregard for the threat and lack of competent forces to conduct security, but most often soft targets are “soft” because of the sheer number of potential targets that exist and the impossibility of protecting them all. Even totalitarian police states have not demonstrated the capability to protect everything, so it is quite understandable that more liberal democratic countries do not possess the ability to provide airtight security for every potential target.

Moreover, some measures required to provide airtight security for soft targets are often seen as intrusive by citizens of countries where personal freedom is valued and the financial cost associated with providing such security measures is often seen as excessive. There is an old security truism that states: “If you try to protect everything all the time you will protect nothing.” Because of this reality, policymakers must use intelligence gained from militant groups, along with techniques such as risk assessment and risk management, to help them decide how best to allocate their limited security resources. While this will help protect the targets the government deems most sensitive or valuable, it will also ensure that some things remain unprotected or under-protected. Those things become soft targets.

While most militants would prefer to attack traditional high-profile targets such as embassies and government buildings, those sites have become far more difficult to attack in the post-9/11 world. At the same time, the relentless pursuit of terrorist operatives by the United States and its allies has resulted in the degradation of the capabilities and reach of groups such as al Qaeda. Today the threat posed to the West stems primarily from grassroots militants and jihadist franchises rather than the al Qaeda core. While this has broadened the threat, it has also made it shallower, since grassroots operatives are far less capable of spectacular and strategic attacks than the professional terrorist cadre of the al Qaeda core.
The combination of increased security at hard targets and the reduced capabilities of militant operatives has resulted in militant planners shifting their targeting toward softer targets, which are easier to attack. As a result of this shift, targets such as hotels have replaced embassies and other hardened sites in militant target selection.

Generally, militants prefer to attack soft targets where there are large groups of people, that are symbolic and recognizable around the world and that will generate maximum media attention when attacked. Some past examples include the World Trade Center in New York, the Taj Mahal Hotel in Mumbai and the London Underground. The militants’ hope is that if the target meets these criteria, terror magnifiers like the media will help the attackers produce a psychological impact that goes far beyond the immediate attack site — a process we refer to as “creating vicarious victims.” The best-case scenario for the attackers is that this psychological impact will also produce an adverse economic impact against the targeted government.

Unlike hard targets, which frequently require attackers to use large teams of operatives with elaborate attack plans or very large explosive devices in order to breach defenses, soft targets offer militant planners an advantage in that they can frequently be attacked by a single operative or small team using a simple attack plan. The failed May 1, 2010, attack against New York’s Times Square and the July 7, 2005, London Underground attacks are prime examples of this, as was the Jan. 24 attack at Domodedovo airport. Such attacks are relatively cheap and easy to conduct and can produce a considerable propaganda return for very little investment.

**Shifting Fire**

In Russia, militants from the Northern Caucasus have long attacked soft targets, including buses, trains, the Moscow Metro, hotels, a hospital, a theater, a rock concert, shopping centers, apartment buildings, a school and now the soft side of Domodedovo airport.
In the case of Domodedovo, the past two attacks involving the facility are a clear illustration of the process by which militants shift to softer targets in response to security improvements. In August 2004, Chechen militants were able to exploit lax security on the domestic side of Domodedovo in order to smuggle two suicide devices aboard two targeted aircraft, which they used to blow up the planes. In response to that attack, security at the airport was increased. The Jan. 24 Domodedovo attack seems to have confirmed the effectiveness of these security improvements — the militants apparently believed they could no longer smuggle their suicide device aboard an aircraft. However, they adjusted their targeting and decided to conduct an attack against a vulnerable soft spot — the arrivals hall — located in the midst of the hardened airport target.

From a tactical standpoint, the attack at Domodedovo was a logical response to increased security designed to keep explosives off aircraft. This attack also demonstrates, significantly, that the militants behind it maintained the intent to hit aviation-related targets, a fixation we have discussed for some time now. One reason for this fixation is the impact that aviation-related attacks have on terror magnifiers. This was seen in the international response to the Domodedovo attacks, which was much larger than the response to twin suicide bombings of the Moscow Metro in March 2010. Even though the Metro bombings produced more fatalities, they did not resonate with the international media as the airport attack did. This media response to the most recent Domodedovo attack was presumably enhanced by the fact that it killed several foreigners.

This difference in international reaction is significant, and will certainly be noted by militants planning future terrorist attacks. In all likelihood, it will also serve to solidify their fixation on aviation-related targets and on soft targets such as arrival halls that are located in the midst of harder aviation targets. It must be noted, however, that this concept is not altogether new: Militants have long targeted the soft area outside airports’ security hardlines. Ticket desks were attacked by the Abu Nidal Organization in Rome and Vienna in December 1985, and more recently the El Al ticket desk at Los
Angeles International Airport was attacked by a gunman in July 2002 and an unsuccessful car bomb attack against the main entrance of the international airport in Glasgow, Scotland, was conducted by a grassroots jihadist in June 2007.

In the wake of the Domodedovo attack, security has been increased in the arrival halls of Russian airports — a step that has been instituted elsewhere in order to make the traveling public feel secure. However, such measures are costly and will tie up security personnel who will then be unavailable to protect other sites. Because of this, these measures will likely be short-lived, and airports will return to “normal” in a matter of months. Furthermore, even when security is increased in areas such as arrival halls, the very nature of airports dictates that there will always be areas outside the rings of security where people will congregate — either to meet travelers or as they wait to clear security screening. While the threat can be pushed away from the airport building, in other words, it cannot be completely alleviated. Because of this, there will always be soft areas that are impossible to protect using traditional security measures. However, facilities that employ non-traditional security measures like protective intelligence and countersurveillance will be able to protect this type of soft area far more effectively than facilities relying solely on physical security measures.

The bottom line for travelers and security managers is that plots to attack aviation-related targets will continue and the array of aviation-related soft targets such as ticket desks and arrival halls will remain vulnerable to attack. A persistent, low-level threat to these targets does not mean the sky is falling, but it should prompt travelers to take some simple steps that can help minimize the time spent on the soft side of the airport. And, as always, travelers should practice an appropriate level of situational awareness so they can see trouble developing and take measures to avoid it.
Travel and Security Risks over Spring Break in Mexico
February 28, 2011

Every year between January and March, U.S. college administrations broadcast warnings to their students reminding them to exercise caution and wisdom while on spring break. All too often, those well-meaning guidelines go unread by the intended recipients. Travel warnings issued by the U.S. State Department may also be disregarded or unnoticed by many other U.S. citizens planning spring trips. Many regular visitors to Mexican resort areas believe cartels have no intention of hurting tourists because of the money tourists bring into the Mexican economy.

This is not an accurate assessment. None of the Mexican drug cartels has displayed any behavior to indicate it would consciously keep tourists out of the line of fire or away from gruesome displays of its murder victims. The violence is spreading, and while tourists may not be directly targeted by the cartels, they can be caught in the crossfire or otherwise exposed to the carnage.

Intensifying Cartel Wars

The Mexican drug cartels have been fighting each other for more than two decades, but this expanded phase, which has pitted the federal government against the cartels, began in December 2006, when newly elected President Felipe Calderon dispatched federal troops to Michoacan to put an end to the cartel violence in that state. With this action, Calderon upset the relative equilibrium among the cartels, and the violence has been escalating and spreading ever since.

The statistics for cartel-related deaths clearly illustrate this acceleration of violence. There were 2,119 such deaths in 2006, 2,275 in 2007, 5,207 in 2008, 6,598 in 2009 and 15,273 in 2010. Statistics compiled from a U.S. State Department database indicate that of the 1,017 U.S. citizens who died in Mexico from 2004 through June 2010,
277 of them died as a result of cartel violence. Notable incidents include the Dec. 30, 2009, abduction and execution of a California school administrator from a restaurant in Gomez Palacio, Durango state, where he and his wife were dining with relatives during their vacation (the victim’s body was found later that day, dumped with five other male victims abducted from the restaurant), and the killing of U.S. citizen David Hartley while in Mexican waters on Falcon Lake on Sept. 30, 2010.

In all areas of Mexico, lawlessness increased significantly during 2010. STRATFOR has often discussed the dangers for any foreigner traveling to such cities as Juarez, Veracruz, Mexicali, Tijuana, Monterrey and Mexico City. In the more traditional tourist resort destinations — such as Los Cabos in Baja California Sur, Pacific coast destinations from Mazatlan to Acapulco, and Yucatan Peninsula destinations centered on Cozumel and Cancun — two distinct but overlapping criminal activities are in play: drug trafficking and petty crime. The most powerful criminal elements are the drug trafficking organizations, or cartels. The main financial interests of the cartels lie in drug- and human-smuggling operations. This does not mean tourists have been consciously protected, avoided or otherwise insulated from cartel violence. The tourism industry itself is not relevant to the cartels’ primary activities, but because the coastal resorts are near cities with ports, which are used by the cartels as transit zones, the battles for control of these ports put resort guests close to the violence.

So while these two main “economic cultures” in Mexico — drug trafficking and tourism — seldom actually intersect, they can overlap. And to make things worse, 2010 saw the cartels greatly increasing their influence over municipal- and state-level law enforcement entities, far beyond previous levels, and corruption among Mexico’s law enforcement bodies has reached epidemic proportions. Today, visitors should not be surprised to encounter police officers who are expecting bribes as a matter of routine or involved in extortion and kidnapping-for-ransom gangs.

This expansion of cartel influence over local law enforcement is evident in the growing number of assassinations and incidents of
intimidation, bribery and infiltration — to the point that many of the local and regional law enforcement agencies have been rendered ineffective. This means wherever law enforcement operates — both in areas where tourists go and in areas where they do not — police officers can be unresponsive, unpredictable and often unwilling to intercede in problems involving residents and visitors alike. That is not to say traditional resort areas like Cancun, Mazatlan or Acapulco have no law enforcement presence, only that municipal police in these cities have demonstrated a thoroughgoing reluctance to get involved in preventing or responding to criminal acts unless it is to their benefit to do so.

This brings into play the second criminal element in Mexico, which is found in tourist-centric areas around the world: pickpockets, thieves, rapists and small-time kidnappers who thrive in target-rich environments. Criminals in this group can include freelancing cartel members, professional crooks and enterprising locals, all of whom have benefited greatly from cartel efforts to neutralize local-level law enforcement in Mexico.

Implications for Resort Areas

What these developments mean for any U.S. citizen headed to Mexican beaches for spring break is that popular locations that until recently were perceived to have “acceptable” levels of crime are starting to see violence related to the drug wars raging in Mexico. Firefights between federal police or soldiers and cartel gunmen armed with assault rifles have erupted without warning in small mountain villages and in large cities like Monterrey as well as in resort towns like Acapulco and Cancun. While the cartels have not intentionally targeted tourists, their violence increasingly has been on public display in popular tourist districts. A couple of recent examples in Acapulco include two incendiary grenades being thrown into a restaurant on Oct. 12, 2010, and the Dec. 17 kidnapping by unidentified gunmen of two employees from the nightclub where they worked. The victims were later discovered shot to death.
Acapulco is a good example of a Mexican resort city turned battleground. There are three distinct groups involved in a vicious fight for control of the city and its lucrative port. Two are factions of the Beltran Leyva Organization (BLO) — one headed by Hector Beltran Leyva, currently known as the South Pacific cartel, the other still referred to as the BLO but consisting of individuals loyal to Edgar “La Barbie” Valdez Villareal. The third group is known as the Independent Cartel of Acapulco. Over the last six months, there have been many grisly displays of severed heads and decapitated bodies left in full view in and near tourist districts. On Jan. 31, federal police in Acapulco arrested Miguel Gomez Vasquez, who allegedly was linked to 15 decapitations in Acapulco in January. On Jan. 9, in the Benito Juarez area of Acapulco, police discovered three bodies hanging from a bridge on Highway 95, a major thoroughfare that leads out of the city to the state capital.

It also is important to understand the risks associated with traveling to a country that is engaged in ongoing counternarcotics operations involving thousands of military and federal law enforcement personnel. Mexico is, in many ways, a war zone. While there are important differences among the security environments in Mexico’s various resort areas, and between the resort towns and other parts of Mexico, some security generalizations can be made about the entire country. One is that Mexico’s reputation for crime and kidnapping is well deserved. Locals and foreigners alike often become victims of assault, express kidnappings (in which the victim can spend a week in the trunk of a vehicle as his or her kidnappers go from one ATM to the next withdrawing all the money in that account), high-value-target kidnappings and other crimes.

Further complicating the situation is the marked decline in overall law and order during 2010, combined with large-scale counternarcotics operations that keep the bulk of Mexico’s federal forces busy, which has created an environment in which criminals not associated with the drug trade can flourish. Carjackings and highway robberies, for example, are increasingly common in Mexico, particularly in
cities along the border and between those cities and Mexican resorts within driving distance.

Other security risks in the country are posed by the security services themselves. When driving, it is important to pay attention to the military-manned highway roadblocks and checkpoints that are established to screen vehicles for drugs and cartel operatives. Police officers and soldiers manning checkpoints have opened fire on vehicles driven by innocent people who failed to follow instructions at the checkpoints, which are often not well marked.

It is important to note, too, that roadblocks — stationary or mobile — being operated by cartel gunmen disguised as government troops have been well documented for several years across Mexico. We have been unable to confirm whether they have been encountered in popular resort areas, but if they have not, there is the strong possibility they will be, given the increase in violence in the port cities. And as violence escalates near Mexico’s resort towns (see below), STRATFOR anticipates that cartels will use all the tools at their disposal — without hesitation — to win the fight, wherever it happens to be taking place. An encounter with a checkpoint or roadblock that is operated by gunmen disguised as federal police or military personnel can be at least frightening and at worst deadly. Driving around city streets in resort towns or roads in the surrounding countryside is becoming increasingly dangerous.

Along with the beautiful beaches that attract foreign tourists, many well-known Mexican coastal resort towns grew around port facilities that have come to play strategic roles in the country’s drug trade. Drug trafficking organizations use legitimate commercial ships as well as fishing boats and other small surface vessels to carry shipments of cocaine from South America to Mexico, and many cartels often rely on hotels and resorts to launder drug proceeds. Because of the importance of these facilities, the assumption has been that drug trafficking organizations generally seek to limit violence in such areas, not only to protect existing infrastructure but also to avoid the attention that violence affecting wealthy foreign tourists would draw.
This is no longer a safe assumption. The profound escalation of cartel-related conflict in Mexico has created an environment in which deadly violence can occur anywhere — with complete disregard for bystanders, whatever their nationality or status. Moreover, the threat to vacationing foreigners is not just the potential of being caught in the crossfire but also of inadvertently crossing cartel gunmen. Even trained U.S. law enforcement personnel can be caught in the wrong place at the wrong time. In Mexico, no one is immune from the violence.

Cancun and Cozumel

Cancun’s port remains an important point of entry for South American drugs transiting Mexico on their way to the United States. Los Zetas activity in the area remains high, with a steady flow of drugs and foreign nationals entering the smuggling pipeline from Colombia, Venezuela, Cuba and other points of origin in the greater Caribbean Basin. There also have been reports that many members of the Cancun city police have been or are on the Zeta payroll. These developments have brought new federal attention to the city, and rumors are circulating that the federal government plans to deploy additional military troops to the region to investigate the local police and conduct counternarcotics operations. At this writing, few if any additional troops have been sent to Cancun, but ongoing shake-ups in the law enforcement community there have only added to the area’s volatility. Though less easily utilized for smuggling activity, Cozumel, Isla Mujeres and associated tourist zones have seen some violence. According to official statistics, cartel-related deaths in the island resort spots off the Quintana Roo coast doubled from 2009 to 2010, from 32 to 64. (For unknown reasons, the government of Mexico’s statistical database does not contain any data for Cancun itself. A quick tally conducted by STRATFOR indicated that approximately 53 executions or gunbattle fatalities occurred in Cancun in 2010.)
Acapulco

Acapulco has become Mexico’s most violent resort city. The Mexican government’s official accounting of cartel-related deaths in Acapulco jumped to 370 in 2010, up 147 percent from 2009. Rival drug cartels have battled police and each other within the city as well as in nearby towns. Suspected drug traffickers continue to attack police in the adjacent resort area of Zihuatanejo, and at least six officers have been killed there within the past two weeks. Between Feb. 17 and Feb. 20, 12 taxi drivers and passengers were killed in Acapulco.

Puerto Vallarta

Puerto Vallarta’s location on the Pacific coast makes it strategically important to trafficking groups that send and receive maritime shipments of South American drugs and Chinese ephedra, a precursor chemical used in the production of methamphetamine, much of which is produced in the areas surrounding the nearby city of Guadalajara. Several of Mexico’s largest and most powerful drug cartels maintain a trafficking presence in Puerto Vallarta and the nearby municipality of Jarretaderas. Incidents of cartel-related deaths in Puerto Vallarta are relatively low compared to places like Acapulco, but there were still 13 in 2009 and 15 in 2010. Threats from kidnapping gangs or other criminal groups also are said to be lower in this resort city than in the rest of the country, but caution and situational awareness should always be maintained. Official statistics of cartel-related deaths for the nearby city of Guadalajara jumped to 68 in 2010 from 35 in 2009, an increase of 94 percent.

Mazatlan

Mazatlan, located just a few hundred kilometers north of Puerto Vallarta, has been perhaps the most consistently violent of Mexico’s resort cities during the past year. It is located in Sinaloa state, home of the country’s most violent cartel, the Sinaloa Federation, and bodies of victims of drug cartels and kidnapping gangs appear on the streets.
there on a weekly basis. The sheer level of violence means the potential for collateral damage is high. The trend upward in the official statistical data is significant. There were 97 recorded cartel-related deaths in 2009, and that number jumped to 320 deaths in 2010, a 230 percent increase.

*Cabo San Lucas*

Located on the southern tip of the Baja California peninsula, Cabo San Lucas and the greater Los Cabos region has been relatively insulated from the country’s drug-related violence and can be considered one of the safer places in Mexico for foreign tourists. Although historically it has been a stop on the cocaine trafficking routes, Cabo San Lucas’ strategic importance decreased dramatically after the heyday of cartel activities there in the late 1990s, as the Tijuana cartel lost its contacts with Colombian cocaine suppliers (the result of joint U.S.-Colombian counternarcotics activities). Over the last five years, drug trafficking in the area has been limited. Still, the southern Baja is part of Mexico, and Cabo San Lucas has ongoing problems with crime, including kidnapping, theft and assault as well as some continuing drug trafficking. Despite the relative lack of cartel violence in the area, official statistics for the greater Los Cabos region show nine deaths in 2010, up from one in 2009.

*Matamoros*

Though Matamoros itself is not a spring break hot spot, we are including it in this discussion because of its proximity to South Padre Island (SPI), Texas. It long has been the practice of adventurous vacationers on the south end of SPI to take advantage of the inexpensive alcohol and lower drinking age south of the border, mainly in Matamoros and the surrounding towns clustered along the Rio Grande. But is important to note that drug- and human-smuggling activities in that region of Mexico are constant, vital to Los Zetas and the Gulf cartel and ruthlessly conducted. On Jan. 29, the Zetas
went on the offensive against the Gulf cartel, and running firefights are expected to persist in the Matamoros area into and beyond the spring break season. Visitors should not venture south into Mexico from SPI.

General Safety Tips

If travel to Mexico is planned or necessary, visitors should keep in mind the following:

• Do not drive at night.
• Use only pre-arranged transportation between the airport and the resort or hotel.
• If at a resort, plan on staying there; refrain from going into town, particularly at night.
• If you do go into town (or anywhere off the resort property), do not accept a ride from unknown persons, do not go into shabby-looking bars, do not wander away from brightly lit public places and do not wander on the beach at night.
• Stop at all roadblocks.
• Do not bring anything with you that you are not willing to have taken from you.
• If confronted by an armed individual who demands the possessions on your person, give them up.
• Do not bring ATM cards linked to your bank account. (Among other things, an ATM card can facilitate an express kidnapping.)
• Do not get irresponsibly intoxicated.
• Do not accept a drink from a stranger, regardless of whether you are male or female.
• Do not make yourself a tempting target by wearing expensive clothing or jewelry.
• Do not venture out alone. Being part of a group does not guarantee “safety in numbers” but it does lessen the risk.

Preparing to Travel Safely  
*July 4, 2011*

With the traditional summer travel season upon the northern hemisphere, the importance of travel security cannot be understated. All travel should begin with an understanding of the risk environment of the intended destination, and contingency plans should be prepared in the event that environment proves too dangerous to stay. We will thus begin our series addressing these issues.

**Before You Travel**

International travel presents certain risks for anyone, especially in areas of the world where the government has limited control over its citizenry and where law and order are not as formally established as they are many parts of the developed world. However, travelers are not immune to risk even in developed countries, as the situation in Greece and the March 11 earthquake in Japan demonstrated. When possible, knowing in advance the cultural and societal differences — not to mention bureaucratic practices that may seem alien to a traveler — as well as the security environment of a destination country provides any traveler the best chance of avoiding risk. With this in mind, appropriate precautions can and should be taken.

Government websites are an excellent place to begin. The U.S., Canadian, British and Australian websites all list travel warnings issued for countries in which potentially dangerous conditions have been identified. They also provide the current Consular Information Sheets of every foreign country, which contain information on visa requirements, health risks, crime, and atypical currency or entry...
requirements. They also list any areas of instability and provide contact information for their embassies and consulates. Moreover, the sites provide a link to a page where travelers can register their personal information at no cost, making it easier for the government to help during an emergency situation. The websites listed above are also useful for non-citizens, as is the information to a traveler regardless of nationality. Notably, for liability reasons, government websites tend to report the worst possible scenario. In other cases, some are outdated and lack specificity with regard to security issues, especially in countries experiencing protests or in smaller countries with a less-pronounced consular presence. Travelers should keep this in mind when researching their destination country.

Travelers should supplement information found on government websites with other sources. Private security consulting firms can provide more customized information tailored to a specific location or client. For those who cannot afford those services, fellow travelers can be great sources of information. Travel blogs and Internet forums can be reliable for “on the ground” intelligence, especially if a traveler has questions about certain locations, transportation or security.

There is an inherent unpredictability in international travel; even the most seasoned of travelers cannot foresee every threat. Knowing as much as possible about the destination country is the best way for travelers to prepare for any situation they may encounter after they embark on their journey.

Mitigate the Risks

Of course, it is impossible to know everything about a location or plan for every possibility, but exercising proper situational awareness is essential for any traveler. Situational awareness necessarily calls for a relaxed state of awareness; constant stress and worry will only make a traveler less capable of handling any problems or risks he or she encounters.

The most common problem a traveler may encounter is street crime — though it is by no means the only threat in many areas of
the world. There are a couple of cardinal rules for travelers to keep in mind if and when they encounter street crime. First, no object or amount of money is worth your life. Most people injured or killed in such robberies resisted their attackers. In addition, travelers should never take anything on their trip they are not prepared to part with, including items of high financial or sentimental value. Thus, a business traveler should always leave backup discs at home and bring along only that which is absolutely necessary for the specific trip to minimize the loss of proprietary information.

In addition, travelers should keep a low profile. It is advisable to dress down while in public and carry less valuable luggage. A cheap watch and a scruffy pair of shoes could be the difference in drawing unwarranted attention to a traveler. Travelers should never carry large sums of money, and larger bills should be broken into smaller bills. Travelers should also use the smallest bill possible when making a purchase. Cash and credit cards should not all be carried in one wallet or pocket but placed in various locations. And it is important to remember that criminals are often satisfied with cash. When possible, identification and other important documents should be kept separate from money, and credit cards separate from cash, so that they do not have to be replaced.

That said, it is important to make copies of passports and other important documents, leaving the originals in a safe location, such as a hotel deposit box at the front desk of a hotel — room safes are not secure. It also is a good idea to keep a copy of the front page of a passport with the relevant identification information along with a list of credit card numbers and contact information for the card companies at home with relatives in case of an emergency.

Relatives, coworkers or friends should be provided a full itinerary before the traveler leaves home — as well as during the trip — so they can provide at least the basic information to the home office or to the appropriate government agency in case of an emergency. In locations where Internet is readily available, it is a good idea to make daily contact with those at home to provide added accountability for
your present and future locations. Buying travelers’ insurance also is a good idea.

Some countries will react negatively or deny entry if a traveler’s passport contains a stamp from other countries. For that reason, many travelers maintain multiple passports, or request that the visa stamp for a particular country be placed on a separate sheet of paper, in order to keep offending stamps separate. Notably, visa and passport information is primarily used by host governments for the purpose of collecting intelligence. There is little the law-abiding traveler can do to prevent revealing such information to a foreign government, absent traveling with a fake passport, which is never advisable.

Preparations such as these can contribute to a traveler’s overall safety during a trip abroad. Arriving at a destination introduces a number of other issues, but being prepared and taking precautionary measures are the first steps a traveler should take to ensure a safe and secure experience.

Air Travel Security
July 5, 2011

On June 24, a dual U.S.-Nigerian citizen named Olajide Oluwaseun Noibi took a Virgin America flight from New York to Los Angeles despite never having purchased a ticket, using a boarding pass with the wrong date and someone else’s name. Well after the flight had taken off with Noibi on board, two passengers seated near him complained to a flight attendant about Noibi’s body odor. After requesting his boarding pass and identification to make alternative seating arrangements, the flight attendant discovered Noibi had illegally boarded the plane, at which point he or she alerted the pilot that a stowaway was on board. The pilot decided to maintain course and keep Noibi under close surveillance, and when the plane landed in Los Angeles the authorities took Noibi in for questioning. (He was
not arrested until several days later, when he attempted to illegally board another flight to Atlanta.)

No evidence suggests Noibi boarded the plane with any malicious intent, and reports since his arrest indicate he has a history of attempting (and on at least one other occasion succeeding) to use a similar ruse to travel. However, his ability to pass through security checkpoints and board a jet without ever having purchased a valid ticket nearly a decade after the 9/11 attacks is an example of how no security system, however well-funded or well-designed, will be vulnerable to human error. For this reason, it is important for travelers to keep in mind the measures they can take to reduce the risks involved in air travel.

**Passenger Awareness as Personal Security**

Since the 9/11 attacks, a number of changes have been enacted to improve security for airline passengers. Air Marshals are present on U.S. and many foreign airlines, cockpit doors remain locked while the plane is in flight and international “no-fly” databases — aimed at ensuring that people who pose a potential threat do not board international flights — have grown extensively. But perhaps the most effective security improvement has been the heightened state of vigilance air travelers have adopted since 9/11.

Situational awareness is always the most important aspect of personal security, and for air travel this entails keeping a number of potential hazards in mind. When boarding an aircraft, passengers should pay attention to the locations of exits, and while in flight count the steps between their seat and the exit. If the plane fills up with smoke, visibility will be impaired, and it is good to know the approximate distance to the exits. If possible, passengers should store baggage in an overhead compartment above or in front of their seat, both to keep an eye on it and make sure it is not tampered with — and to make disembarking quicker.

Communication is important between passengers and flight attendants; it is also important between passengers. If something seems
unusual with another passenger or the plane itself, telling someone can help bring attention to a potential problem. Indeed, without passengers contacting the flight attendant in the Noibi case, his status may have gone undiscovered.

There are also a number of relatively inexpensive items passengers can purchase that could be useful in an emergency situation. Examples of these include a smoke hood (a protective device that prevents smoke inhalation) and a small flashlight among a passenger’s carry-on items that can be utilized in an attack or an accident aboard the aircraft. In such situations, smoke inhalation, especially from the extremely toxic burning plastics within a plane, poses a serious threat. In addition, a flashlight can be used to facilitate a passenger’s leaving an aircraft when the power is out and the air is thick with smoke. Such emergency gear should be kept in a pocket or in a bag kept at the passenger’s feet.

‘Hard’ vs. ‘Soft’ Security

With more emphasis placed on securing aircraft in recent years, potential attackers may attempt to attack terminals rather than the planes themselves, where crowds of waiting people present an enticing, easier-to-attack target for militants aiming to cause mass casualties. It is useful to think of airport terminals as divided into two parts. The “soft side” is the area near a ticket counter and, in the case of the United States, before Transportation Security Administration checkpoints, where passengers and carry-on luggage are screened — while the “hard side” is past the security checkpoint. Time spent in line at the ticket counter and at security checkpoints should be minimized when possible, though as all air travelers know, this is often easier said than done.

In the first case, arriving at the counter early enough (three hours for an international flight, two for a domestic flight) to avoid the rush of latecomers generally reduces the amount of time one will spend in line, and thus the time one is vulnerable to an attack. Airports are set up to minimize loitering in the soft area for this reason, among others.
To expedite the process, one should avoid wearing clothes with lots of metal buttons and buckles and shoes that are not easily removed. One should also minimize the amount of carry-on baggage he or she may bring on board. It is likewise important to have all travel documents somewhere easily accessible, such as a folder or travel pouch. The January 2011 attack against Moscow’s Domodedovo airport is a prime example of an attack against the soft side of airport security and illustrates the need to minimize the time spent outside the more hardened area past security checkpoints.

Once on the hard security side, travelers should attempt to avoid the congested waiting areas at the gate, if possible, by utilizing the members-only lounges operated by many airlines. This helps to keep the traveler out of a potential attack zone, away from crowds and out of plain view.

Passengers using airport wireless Internet services should be careful to only connect to the airport’s official wireless hub and avoid using public networks for anything deemed sensitive — banking information, anything involving a social security number or work-related confidential information, to name a few. If Internet use is necessary, do not connect to access points named “Free WiFi” as it may connect to a hacker via a computer-to-computer connection, making the user vulnerable to identity theft. Also, newer generation cellular phones may automatically connect to available access points, making them vulnerable to a hacker trying to steal personal information. This function usually can — and should — be turned off before arriving at the airport.

**International Travel**

In many parts of the world, air travel can be dangerous because of inadequate safety, maintenance and security procedures. This is especially true in the developing world, where maintenance regulations and procedures often are not strictly enforced. The U.S. Federal Aviation Administration (FAA) prohibits U.S. carriers from flying into foreign airports that do not meet security and safety standards.
HOW TO TRAVEL SAFELY

Although this information is not readily available to the public, determined travelers could contact the FAA for a list and then avoid those airlines and airports that are considered substandard. The consular information sheets issued by the U.S. State Department also provide information about air travel safety. In addition, airport terminals, especially in the developing world, are notorious for criminal activity. When on the soft security side, unattended luggage can be stolen, and travelers can be victimized by pickpockets — especially when they are less vigilant after a long, exhausting intercontinental flight.

At the destination airport, transportation can be arranged in advance to further minimize time spent on the soft side of security. For traveling executives, discretion should be employed in finding the local driver on the other end of a flight. A driver who holds up a sign bearing the executive’s name and company could tip off potential kidnappers or militants to the presence of a high-value target.

Situational awareness and preparation are the most effective personal security measures a traveler can take to avoid this and other potential hazards. Paying attention to people and events in the area and avoiding potential attack zones are two basics for self-preservation while in the terminal and on the plane.

Hotel Security

July 6, 2011

On July 1, at 7 p.m. some 1,500 guests at the Park Lane Hilton in London were forced to leave the hotel when a basement fire spread to the hotel’s second floor. Firefighters were able to extinguish the fire, and no fire-related injuries were reported. Three days later, a shooting at the Doubletree Hotel in Memphis, Tennessee, left one guest dead and one of the two responding police officers dead after he separated from his partner to find the assailant.
That two people were killed during the Doubletree shooting is regrettable and should not be understated. However, both situations had the potential to be much worse than they were — in terms of human casualties — and are all the more reason for travelers to understand the various emergency situations they may encounter while staying at a hotel. Knowing what information is needed and what steps should be taken in those situations will give a traveler the best possible chance of survival. STRATFOR has written extensively on militant threats to hotels as well as steps a traveler can take to mitigate those threats. It is important for travelers to recognize the personal security issues relevant to a typical hotel stay.

Avoid the Chaos Factor

Typically, the largest threat to a traveler in an emergency situation is chaos. People's instincts to protect themselves can lead to unpredictable and, at times, dangerous behavior when their survival is at stake. This is why it is even more important to plan for and practice emergency situations, especially in places like office buildings or hotels, where confusion and fear are compounded by the unfamiliarity of the location and the people around you. Preparation, common sense and situational awareness remain the most important aspects of personal security anywhere; personal security at a hotel is no exception to this axiom.

Before even making a reservation at a hotel, a traveler should first learn whether it has enacted adequate security measures. This information is best acquired from a trusted business associate or other source in the country, rather than the hotel itself, which could provide hollow assurances. After all, a hotel has every reason to want to retain your business at the expense of a competitor, even one with superior security.

Most Western hotel chains have safety protocols for emergencies, and the employees for those hotels are trained and competent in security procedures. Government agencies in Western countries will, for the most part, respond promptly and reliably to emergency situations.
Equipment such as fire alarms, water sprinklers, closed-circuit television cameras and emergency exits all function properly. But, for these reasons, a traveler tends to take his or her safety for granted, trusting that others will come to the rescue in case of an emergency. This creates a false sense of security because it is impossible for hotel staff to watch everyone at all times. Closed-circuit television cameras are valuable only if someone monitors them at all times (and if someone is available to promptly respond to an emergency), which is often not the case.

In the developing world, travelers must take even more responsibility for their security. Some hotels, especially in small towns, may have no security measures or procedures in place at all. The security equipment they may have, such as metal bars on windows, can actually cause more harm than good, and sprinklers and fire extinguishers may be inoperable. Buildings are typically not built to Western fire code standards, locks on doors may be easily picked or manipulated, and hiring practices can be substandard, especially when the hotel does not have the wherewithal to perform thorough background checks for potential employees.

There are some measures a traveler should take no matter where their hotel is in the world. When choosing a hotel room, the room should not be so high that an extension ladder could not reach it in the event the hotel is evacuated. Standards on ladder lengths vary, but the second through fifth floors generally are acceptable. Moreover, it is important to take note of fire exits in a hotel in case of an emergency event. A traveler should physically walk the exit route from a room to safety to verify that doors and stairwells are unlocked and free of obstructions — locked doors and obstructions can occur both in developed and developing countries. Because smoke inhalation is the most common cause of death in a fire, having a flashlight, smoke hood and cell phone at the ready is recommended at all times. Absent a smoke hood, a traveler should cover his or her mouth with a wet towel and remain low to the ground. Hotel guests should also bring along a map of the premises when they flee the building (many hotels
provide such maps on the doors of their rooms). If traveling with others, a person should have a designated rally point outside the hotel.

**Personal Safety Precautions**

Fires are by no means the only threat a traveler may encounter during a hotel stay. Theft, kidnapping and other attacks present real threats to a traveler’s security, and measures to counter such threats abound.

When possible, a guest should choose a room location above the ground floor of a hotel, decreasing the room’s accessibility to criminals. Once inside the room, a guest should avoid opening doors to unannounced visitors, all of whom should be told to wait in the lobby so the front desk can verify their identity and reason for being there. Most important, a guest should ascertain whether someone has a reason for knocking on the door and asking for entry. When in doubt, do not open the door.

A traveler should accept at least two keys when checking in to the hotel, and he or she should clarify to the front desk who is allowed to receive a key if one is lost or stolen. A traveler should also avoid returning their room key to the front desk — this allows people to easily see that a room is unoccupied. It should be kept in mind that a room safe is not safe, so a traveler is better served keeping important valuables on his or her person or at a secure location at the front desk.

Security door locks should be used at night, and the door should never be propped open when going out — a thief needs only a small window of opportunity to enter a room. For the frugal traveler, an inexpensive wedge door lock (a rubber wedge placed between the floor and the bottom of the door) can also provide added security.

Cleaning staff should not be allowed into the room in the absence of the guest, and the “Do Not Disturb” sign should always be placed on the door handle to discourage anyone from entering the unoccupied room. Whether the hotel staff is complicit in criminal activity or not is irrelevant; a discerning traveler should minimize access to his or her hotel room at all times so that complicity is never a factor.
If driving a car, a traveler should park only in hotel parking lots that are well lit — preferably near the lobby or in a spot visible from the hotel room. When walking in the parking lot, a traveler should have the keys in hand, always checking inside the car before getting in. Valuables should be kept out of site or in the trunk of the car, as thieves are more likely to target a car known to contain valuable items.

In some countries, such as China, hotels are used to gather intelligence on guests. Using Internet services at a hotel can make a guest’s computer vulnerable. A traveler should assume telephone conversations on hotel lines are tapped and rooms are bugged for sound — and probably video. He or she should never leave a laptop, PDA or important documents in the room when away because the devices could be stolen, cloned or copied.

Hotels — often erroneously — are seen as a secure location where the every need of a traveler is cared for, from turning down his or her bed to ensuring his or her personal safety. Indeed, hotels try very hard to make a guest feel at home; the onus of the guest is to remember that he or she is not. A false sense of security can lull a traveler into letting his or her guard down and abandoning the state of relaxed awareness needed to practice personal security when traveling.

---

Public Transportation Security

*July 7, 2011*

International travel necessarily entails logistical concerns — scheduling flights, tracking luggage, finding accommodations. Indeed, it can be easy to forget that such travel does not end when a traveler arrives at the airport of his or her destination country. Once a traveler has arrived, he or she must get from one place to another within the country — an act that presents entirely new risks to a traveler.

In general, it is safer to use low-profile private transportation than public transportation when traveling abroad. Safety, however,
is not the only consideration most travelers have when planning to get around in their destination country. Money and convenience also play a part, in which case they may want to consider using public transportation. Regardless of the reasons public transportation is used, the risks involved in utilizing public transportation remain. In this installment in our series on travel security, we will explain these risks and the ways in which travelers can protect themselves while using public transportation.

What to Expect

The majority of crimes committed against travelers using public transportation in foreign countries are not violent but petty, such as pickpocketing. (That is not to say serious crime is unheard of; in Tokyo and Cairo, women-only subway cars are maintained to prevent women being groped, a huge problem in those cities.) In fact, airports, subway trains and stations and bus stations all over the world are notorious for pickpockets, as criminals look to prey on tired and disoriented travelers. The simplest and most frequently used tactic in these locations is the “bump and grab.” In this tactic, pickpockets will misdirect their victim’s attention while removing a wallet from a pocket or backpack. Other methods involve the criminal using a razor blade to cut the bottom of a backpack or purse and removing the contents within, especially if the thief has observed a person putting their money in the bottom of a bag where they think it is safest. The “grab and run” is also a popular method, especially if a person has put their purse or laptop bag on their shoulder and not across their body, or left it on a chair next to them.

On a bus or a subway car, travelers can fall victim to all manner of schemes. In Guatemala, for example, pickpockets frequently target foreign travelers packed into old school buses — the country’s version of municipal buses. Many travelers keep valuables in side pockets and in cargo pockets, which criminals will cut open to remove the contents. Baggage stowed under a seat is liable to be stolen by a thief sitting behind the owner. In some instances, thieves will take a bag
How to Travel Safely

from an overheard bin and quickly throw it out the window to an accomplice. It is not uncommon for street gangs to board buses and demand a tax be paid for passage through their territory — although they usually target the bus drivers. Moreover, buses and private shuttles also can be targets for criminals in rural areas where there is little or no law enforcement presence.

Travelers can counter these threats in a number of ways. The best place to put a bag is above or in front of the seat if possible, with other valuables placed in the lap. Important documents should be located on a traveler’s person, separate from money and other valuables. They should always keep important items well inside their bag, rather than in the outer pockets, especially in the top section of a backpack. Travelers should wear a smaller bag or purse across the shoulder and position it in front — men can place a smaller backpack with important documents on their chests instead of their backs. It is a good idea to keep small locks on bags because despite being seemingly easy to break, they deter theft by causing a criminal move on to easier targets. When exchanging money for a ticket or fare, a traveler should take care to not flash all his or her money at once — this is a surefire way to get unwanted attention. Travelers can keep a small amount easily accessible in a front pocket for small purchases but can keep the bulk of their money hidden elsewhere. Also, if a traveler is forced to evade criminals, keeping in mind possible safe areas — a ticket booth in a subway, for example — is highly advisable.

It should here be noted that airports and bus and metro stations are prime targets for terrorist attacks. These locations both offer militants the opportunity to inflict mass casualties and allow them to attack specific groups, such as U.S. tourists on their way to see a historic site or Israeli soldiers waiting at a bus station in Tel Aviv. Thus, situational awareness, the knowledge of how to identify threats and communication with employees or other passengers is critically important.
Taxis

Taxis present a problem for travelers all around the world and should only be used if deemed safe by an associate or trusted local. Taxi drivers pose a number of threats, some of which, like overcharging for a ride, are relatively benign. Other, more sinister ones involve actively helping a criminal gang rob or conduct an express kidnapping on a traveler.

Taxi drivers, by nature, are in a position of power because they know where they are going and how much the ride should cost. One way to mitigate the driver’s power is through preparation prior to the ride. This can be done by researching travel blogs, contacting a hotel or asking business associates and contacts in country. A traveler should only use official taxis. Many cities will have designated taxi stands where a person can go to hail a taxi. A traveler can often get an estimated fare from this stand. It is generally advisable to never hail a taxi from the street. In some places, such as Mexico City or San Salvador, hailing a cab in such a manner makes it easier for kidnappers to grab a person standing on a curb.

A traveler should never take a “black” taxi, which can be an unofficial taxi or even a normal car. Not only is it illegal to do so, it also puts a traveler at risk for crime. Moreover, the drivers themselves run the risk being assaulted by official taxi drivers who see black taxis as an encroachment on their business. When getting in a taxi, a traveler should check to see if the door locks and the windows are operable. A traveler should never allow the driver to bring along a “brother” or “friend” — such a scheme is likely a prelude to an attack. More often than not, there will be metered taxis in a country. A traveler should never use a taxi if the driver refuses to turn on the meter, and if there is a question about the price in most developed cities, asking a witness at the final destination how much a taxi ride should cost is a good way to avoid being overcharged. In places where taxis do not have meters, a traveler should negotiate the price beforehand.
Alternatives

There are alternatives to public transportation. As stated before, using private transportation is generally safer than using public transportation. Cars and drivers can be hired in advance, upon recommendation by reliable local sources, other travelers or business contacts. Hotels can also make recommendations for private drivers or accredited taxi companies. A traveler can usually trust these drivers because they likely have a longstanding relationship with the hotel — they would not want to jeopardize that relationship by putting the passenger in danger. Private transportation is expensive, however.

Detailed and customized information about specific threats to travelers overseas can be obtained by utilizing a private security consulting firm. In addition, consular information sheets provided by the U.S. State Department and similar services provided by the British and Australian foreign ministries list common crime and/or transportation problems for particular countries.

As always, situational awareness is the key to being safe and protecting ones property. A traveler’s awareness of the risk environment he or she is in can prevent risks before they occur — listening to music loudly with headphones or having one’s nose in a book is generally inadvisable. Even in relatively safe cities, absentminded travelers can fall victim to petty crime on a subway or bus. Travelers are best served making an ally or friend, be it the bus driver or someone in a nearby seat. In some cultures, such a relationship can foster a sense of responsibility in the local. Whatever the case, a traveler appearing likable will prove beneficial in the event he or she falls victim to the risks of public transportation.
Mitigating the Threat of Street Crime

July 8, 2011

Part of the allure of international travel involves walking the streets and seeing the sights of an unfamiliar locale. Whether it is done for professional or recreational reasons, venturing out onto the streets of a foreign city is inherently risky for visiting foreigners.

Criminal elements in developed and developing countries alike tend to target travelers — Westerners in particular — because of a general belief that they carry or have access to large sums of money. Whether this belief is accurate or not is irrelevant; that criminals hold this belief renders a traveler a tempting target for criminal activity. Therefore, travelers can and should take a number of precautions to avoid being the target of street crime.

Minimize the Risks

A traveler should understand the culture in which he or she is traveling. What may be an appropriate response to a potential crime in one country may be completely inappropriate in another — a point to which we will return. Cultural differences notwithstanding, no amount of money is worth a person’s life. A traveler should concede his or her money or possessions during a robbery rather than risk violent reprisal from the culprit.

If a traveler believes he or she is under surveillance from a potential thief, an effective way to deter the criminal is by making eye contact. When doing so, a traveler should not act aggressively or maintain eye contact for more than a moment. If a suspicious person indeed has malicious intentions, he or she will likely move on to an easier target for fear of being made. A traveler should immediately move to a safe location if the criminal is undeterred by eye contact.

In fact, such safe locations should be noted while a traveler walks about the city streets. They should be secure locations that can be entered quickly — small cafes and shops are two examples of such locations. Most locals and proprietors will disapprove of and
discourage a criminal’s attacking potential clientele. Banks, auto shops and some hotels are even better locations because they usually employ security personnel, who may even be armed.

Travelers can employ a number of other measures to minimize the risk of attack. Walking about unfamiliar streets while listening to music generally is inadvisable because it lowers a traveler’s situational awareness. In many countries, an iPod or iPhone, for example, can equate to a month’s wages for a local. In addition, exploring the streets in groups is better than doing so alone. Criminals may target a group in hopes of a larger payout, but they will usually avoid them because such targets increase the chances of a criminal’s detection.

When renting a car, a traveler should request an older model to keep a low profile. New and luxury cars, especially those driven by foreigners, are prime targets for car thieves and kidnappers.

Male travelers looking to commingle with female locals need to be aware of one piece of advice in particular: If beautiful women do not approach a given man in his home country, the chances are high that any woman who approaches him in his destination has ulterior motives. It is a common tactic, in places as different as Budapest and Miami Beach, for a beautiful woman to ask a Westerner to buy her a drink — at a highly inflated price. After receiving the bill, the victim will be forced, often by much larger men, to withdraw enough money from an ATM to cover the bill. In China, the “tea room” scam is a variation of this scenario. A young man or woman will ask a traveler if they would like to have a cup of tea, only to take him or her to a location where a pot of tea costs an exorbitant amount of money. Many travelers will neglect to ask for prices beforehand, something that should always be done when traveling.

Prostitution, aside from generally being illegal, also can facilitate crime in many countries. Prostitutes can be used to lure a victim into a location where kidnappers or thieves are waiting, or they can drug victims in order to rob them, so good judgment should be used when accepting a drink from a stranger.

One way to have an effective countermeasure to criminal activity is to make an ally or friend wherever possible. When dining at
a restaurant or bar, a traveler should have a conversation with the bartender or waiter. Courtesy goes a long way in many cultures, and if a traveler falls victim to criminal activity, he or she benefits from having someone who knows or remembers him or her. In parts of Africa, for example, a kind word to a bus driver can engender a sense of responsibility for a traveler’s well being.

In cases of kidnapping or violent assault, a traveler must be able to decide at a moment’s notice whether to fight or submit to an assailant. So many factors come into play in such scenarios that it is difficult to generalize a standard procedure — training of the target, at what point in the attack cycle the assault was identified, and the type of force employed against the target. The intent of the assailants is also important. The dynamic of locations in which kidnappings occur frequently or where hostages are killed for political theater is much different than that of locations where express kidnappings are the norm. In short, there is no standard for countermeasures for an attack; they should be determined on a case-by-case basis.

Perhaps the best way for a traveler to avoid being targeted for a crime while abroad is to maintain a low profile — wearing casual clothing, inexpensive jewelry, shoes and bags. Donning flashy accessories or pulling out large amounts of cash will invariably draw attention to a traveler. If a traveler must bring along large amounts of money, he or she should keep it separated rather than in one wallet or purse. A moderate amount of cash — the equivalent of $25-$50, for example — kept in one’s front pocket can be handed over to a thief without incident or regret, keeping the duration of the confrontation to a minimum.

Foreign travelers tend to focus on their vacation or business trip when they should be thinking about their inherent vulnerability. Many countries in the world can be overwhelming for travelers, so a few minutes of observation can ease their state of mind. They should find a place to survey their security environment, particularly in situations where they are spending money.
Monetary Transactions

Travelers need to exercise extra caution when withdrawing money from ATMs, especially when location makes a difference. The best place to use an ATM is in a secure location, such as the inside of a bank or hotel lobby (because many banks are surveilled by criminals, travelers should put away the money they withdraw before leaving the building). Many hotels abroad also will process cash advances from the traveler’s credit card account or exchange U.S. dollars into local currencies. Traveler’s checks also can reduce dependence on ATMs. The key to avoid using ATMs at risky times or in risky locations is to plan ahead and to have the correct amount of cash needed for the day’s or night’s activities.

Another way for a traveler to mitigate the threat posed by withdrawing cash — not to mention that posed by express kidnappings — is to travel with a prepaid bank card, acquired from his or her own bank with a small, finite amount of cash. Also, having the bank card’s international assistance number in a secure location is helpful in the event an ATM card is stolen.

An increasingly prevalent type of fraud at ATMs is known as “skimming.” This involves placing a device that looks like part of the machine over the card slot. The device contains a card reader that records account information when the ATM is used, allowing cyber-criminals access to bank account information. In other instances, a camera is placed on the machine to record PIN numbers.

The exchange rate in some countries, which can be artificially skewed in the host country’s favor, could tempt some travelers to engage in informal currency exchanges on the street or in established places of business that are unauthorized to exchange cash. Visitors who participate in such illegal practices put themselves at risk of deportation or incarceration. This practice exposes the traveler to the risk of receiving counterfeit money, which in turn puts the traveler at risk when he or she tries to use the money. It is not unheard of for business executives, having been apprehended exchanging money on
the black market, to be blackmailed by foreign governments, who force them to commit industrial espionage on their companies.

Moreover, exchanging money on the street can put the traveler in close proximity with the local criminal element, which is often tied to organized crime. What begins as an informal money exchange can easily evolve into a kidnapping scenario. If the exchange rate offered by someone on the street sounds too good to be true, it usually is.

There are inherent risks involved when a foreigner wanders the streets of an unfamiliar city. However, travelers can reduce the chances of becoming a victim by being aware of their surroundings and taking certain precautions.

Protecting Sensitive Information in Electronic Devices When Traveling

July 9, 2011

German business magazine Wirtschaftswoche on June 25 reported a novel counterespionage technique used by the board members of a German chemical company, Evonik. In Evonik’s executive meetings at the office, everyone must put their cellphones in a metal tin — essentially a cookie jar — to block the phones’ signals and possibly to block their microphones as well. Mobile devices can be accessed remotely via malicious software, known as malware, turning them into listening devices, but the right tin can will act like a Faraday cage to block mobile signals. Evonik’s technique works, with some exceptions, if the executives’ only security goal is to stop someone from listening in on their meeting. Evonik’s executives are operating under a correct assumption: Mobile devices are easily compromised and present an information-security risk.
The Risks to Mobile Devices

Mobile devices are more vulnerable to criminals when traveling, particularly in unfamiliar places. Business travelers often depend on devices such as laptops, mobile phones, PDAs or tablet computers. They also carry mobile storage devices, such as USB keys, MP3 players and external hard drives. Travelers who fail to secure these devices while traveling abroad expose the devices and the information they contain to data theft and infiltration by malware that can be installed on the device.

Travelers’ devices also are vulnerable to physical theft. Criminals target laptops and smart phones for their high resale value. These devices are frequently stolen in airports, bars and restaurants as well as on trains and buses — and even in the street. Laptops and mobile devices should not be set down anywhere a thief can quickly snatch it and run. Even carrying a laptop or mobile device in something other than its case, such as a backpack or a buttoned pocket, will push a criminal, who is looking for the easiest target, to go after someone else.

There are more risks, however, than physical theft. Private competitors or foreign governments may seek to access devices in order to glean valuable company-specific information such as client lists, account numbers and, most valuably, intellectual property.

Some countries use their national intelligence services to spy on visiting executives, especially when the executive’s competition in the host country is state subsidized or the technology involved is considered a national priority by the host government. This makes the visitor’s information vulnerable not only to hostile intelligence, but to hostile intelligence backed by state resources, which are significantly greater than those of corporate spies. This has been known to occur in Russia, India and China as well as in countries that many executives might not consider hostile, such as France and Israel.
Protecting Data

Commercially available encryption programs can help protect sensitive information on computers when traveling. But the program’s password should never be saved on the computer; in fact, it is best to avoid saving any passwords, or at least to use different and more secure passwords for important accounts. In addition, icons for the encryption program should not be displayed on the desktop or task bar. Airport security personnel in some countries have been known to start up a visiting executive’s laptop and, upon finding a software encryption program icon, have attempted to retrieve the computer’s data and have even damaged the computers when they could not gain access. For another layer of assurance, entire or partial disk encryption minimizes the exposure of data and takes the burden off the user to manually encrypt and decrypt files and folders.

The best way to protect sensitive information contained on a laptop or mobile device is to avoid exposing it to potentially compromising situations. The computer should only contain information specific to the current trip and, when possible, should not contain account numbers, passwords or other sensitive information. Then, should the device be compromised, the executive can take some comfort in knowing that not all of the company’s sensitive information has leaked out. When traveling, it is best to replace the regular computer or hard drive with a clean one. This helps protect the data abroad and avoid compromise when the trip ends. The methods described below, used to access a traveler’s electronic device, can also be used to plant malware that will extract information through online networks only after the users returns to their office.

It also is important to ensure that all important data on a laptop is backed up in another location. In high-crime areas it is advisable to carry data in an external hard drive or a mobile storage device, separate from the rest of the computer. This approach involves security concerns of its own, outlined below. However, should the laptop be stolen, the thief will not get the data, which is likely far more valuable to a traveling executive than the machine itself.
In some countries, the local intelligence service may try to access laptops or mobile devices left in an executive’s room in order to extract data or place malware. They may even steal the devices to make the incident look like a common theft. For this reason, laptops and mobile devices should never be left in a hotel room, or even in the room’s safe — especially in a country in which the government needs only to ask for a key from the hotel.

Ensuring the constant, physical security of mobile devices and computers is necessary to effectively secure important information. Executive protection personnel should take custody of a traveling executive’s electronic devices when they are not in use — for instance, while the executive is making a speech or attending an engagement.

One alternative is to carry only a smart phone or tablet computer, especially if it can be done without carrying sensitive information, and only used for less-sensitive email communication through encrypted servers. These devices are smaller and easier to carry at all times. But wireless devices have their own inherent security risks and are still vulnerable to theft. Moreover, mobile devices are not nearly as secure as laptops and usually do not encrypt their data.

The prevalence of information breaches over computer and phone networks may make some of this advice seem less important. Yet while networks provide access across continents, devices in physical proximity remain much easier to breach. The basic ability to intercept signals, which criminals can easily do on Wi-Fi networks, is a concern for all encrypted communication, and it is undetectable because it intercepts the data on radio waves rather than by infiltrating the computer. Even the best-encrypted communication has its failure points. One simple and important way to mitigate the risk of compromise is to turn off all network interfaces until they are needed. Most laptops and mobile devices leave Bluetooth on by default, and this is often easily compromised in its standard configuration. Other interfaces like infrared, GPS radios and 2G or 3G radios should be disabled to avoid the risk of compromise or tracking via tower triangulation.

When traveling in a country considered hostile or known to be involved in corporate espionage, a traveler should assume that all
communications networks, both wired and wireless, are compromised. Researchers have demonstrated how GSM phone networks can be compromised using a few phones, a laptop and the right software. A virtual private network (VPN), which many companies use to partially encrypt their communications, is best used for email and similar communications. Individuals can set up their own VPNs fairly easily at no cost.

**Countermeasures**

Any traveler, from a student to an executive, can take key preventive measures to help ensure security. An individual can help prevent compromise by locking devices and requiring password access; not installing software, particularly mobile applications, from unknown developers; diligently installing software updates; and not accessing sensitive information, particularly bank accounts, through mobile devices. It is never a good idea to check bank accounts through a mobile device’s browser — a trusted application from the individual’s bank is a better idea — and the same applies to company email and other communications that should remain secure. Consider that with all advancing technology, security is a step or two behind. Smart phones in particular are running on new operating systems. This means that mobile devices are often more easily breached than computers.

Even when a traveler or executive takes all available security precautions, vulnerabilities still exist. For example, RSA, the security division of EMC Corp., has specialized in data security, particularly secure authentication for network access including using mobile devices, since creating the first public security key algorithm in 1977. The March 2011 infiltration of RSA, and subsequent infiltrations of L-3 Communications Corp. and Lockheed Martin Corp. using information on RSA’s security tokens, demonstrates that the most secure data can be breached. RSA provides secure authentication for network access, including using mobile devices.
Laptops, tablets, smart phones and other mobile devices have become essential travel accessories. They hold a vast amount of information in a relatively small space and offer easy access to communications. For this same reason, these devices and the information they contain are very valuable for anyone with hostile intentions. Travelers who safeguard the information on these devices and take precautions to mitigate the effects of a compromise could be sparing their companies serious harm. If possible, travelers should go without their usual electronic devices. A company can designate certain laptops for foreign travel, to be sanitized by an IT department or contractor on return. Any mobile storage devices, which can easily carry malware, should also go through such a sanitation process, and disposable phones can be purchased overseas.

Of course, this advice may seem impractical. Given the number of vulnerabilities, it is always best to assume electronic devices and data are compromised. The surest way for travelers to protect their electronic data is to keep the most important information in their heads, offline or in secure storage.

Common Sense When Traveling Abroad

July 10, 2011

This travel security series aims not to frighten readers, but to prepare them for travel and everyday life abroad. Traveling abroad is generally a positive experience, and while travelers who leave their comfort zone for a foreign land should be aware of their surroundings, they should not feel fearful or paranoid — which can actually be counterproductive to good security. While there are risks, travelers who exercise proper situational awareness and follow the basic rules outlined in this travel security series, can enjoy the experiences and perspective traveling offers.
It is always important that travelers take time to observe and think before acting. A traveler can learn a tremendous amount about a location and its customs by paying attention to the surrounding environment. Travelers should make a conscious effort to study their environment in an effort to determine what is normal — and what is not. If something feels wrong, even subconsciously, it probably is. This process also works in an emergency: first in recognizing the threat, then understanding it, making a plan to address it and finally acting to either counter the threat or escape the situation. Finally, a traveler must trust his or her instincts about what is normal and what is anomalous or even potentially dangerous.

**Be Smart**

Travelers who engage in illegal activity while abroad can find themselves in serious trouble. These activities naturally bring travelers in close contact with criminal elements, increasing the potential for threats. Moreover, if the traveler is caught and arrested, he or she becomes open not only to criminal prosecution but also to extortion by corrupt elements of the local police. Local law enforcement officials in many countries literally have the power of life and death over people who break the law in their jurisdictions. They can be just as likely as a criminal element to beat, rob or even kill someone in their custody. Business people can even be blackmailed by intelligence services into giving up company trade secrets or committing treason against their country.

Ignorance of the law is never a defense, nor is the idea that “everyone else is doing it.” It is the traveler’s responsibility to know the law and culture of a travel destination. Illegal activity is no less illegal simply because others are observed engaging in it.

Westerners must understand that if they are arrested, the police may not care where they are from. No traveler, regardless their country of origin, has the right to be belligerent or break the law. Nationality will not save someone from the consequences of their actions. In fact, depending on the crime and other factors outside the traveler’s
control — such as politics and international tensions — nationality can prove a liability. A traveler’s embassy can make sure an arrested citizen is not subjected to human rights violations or abuse, but it will not be able to save a person who has broken the law.

When abroad, it is common for travelers to want to take part in local entertainment. Such activities can lower the traveler’s guard, especially if alcohol is involved. Add to this a prevalent feeling among travelers that they are allowed to behave in ways normally unacceptable in their home countries, and it can be a volatile mix. While some tourist locations allow some leniency regarding public drunkenness or disorderly conduct, it is a mistake for travelers to think they can act without consequences.

Bars and casinos, especially those that facilitate prostitution or drug trafficking, can present several threats. Travelers could find themselves in the middle of an illegal transaction or armed confrontation between gangs. Furthermore, a traveler who is convinced to engage in a sexual liaison may find that their companion has accomplices lying in wait to commit a robbery — or worse.

Street vendors or other locals may also be looking to make a victim out of an unwitting visitor by offering to escort the foreigner someplace to look at merchandise or to meet local artisans. These scenarios sometimes end in a bad part of town where accomplices are waiting to commit robbery or cause bodily harm.

Children are known to be expert pickpockets in many countries. They often surround a traveling Westerner, seemingly to talk or ask questions, but in reality to remove his or her possessions. Adult criminals will also use children as a diversion.

Criminal elements also will take advantage of a visitor’s lack of familiarity with local geography and customs. Travelers who walk around a foreign city with the idea of taking in the local color risk wandering into a dangerous neighborhood. Every city has areas that are dangerous for local inhabitants, let alone conspicuous strangers. This risk can be compounded when the wandering occurs at night, even when travelers are in a small group.
To keep a low profile, visitors should dress modestly, especially in a conservative or religious country. They should also know local customs before dressing in native clothing; certain colors and patterns have special, subtle meanings in native cultures. Missing these meanings could be offensive to these cultures — and dangerous for the traveler. Also, wearing a jersey or other clothing representing the wrong sports team, such as a soccer club, in the wrong location can lead to violence.

The desire to videotape or photograph travel memories also can lead to problems for travelers who are unaware of local laws and customs. In many countries, it is forbidden to photograph military installations or government buildings. Security forces also can take offense when being photographed, and in some parts of the world may respond by confiscating film, breaking cameras or worse. In many countries, photographing civilians, especially children, can be considered offensive behavior. This is especially true for locals taking part in religious rituals. They may react negatively, perhaps even aggressively, to even being asked to be photographed by an outsider.

To avoid trouble abroad, travelers should use common sense and always maintain a high state of situational awareness. The same general rules apply to any city around the world: Avoid hustlers, muggers, gangsters, pimps, grifters and pushers.

When preparing for a trip abroad, travelers should consult consular information on the destination country. This document, as well as any recent warden messages from their home countries’ embassies, will contain information on potential threats and recent trends in local criminal activity. For further information about generally safe places to visit (as well as those to avoid), the concierge in most quality hotels can be a reliable, knowledgeable guide. In some cities with critical crime or terrorist threats, it might even be advisable not to leave the hotel or resort property at all during leisure times, especially after dark. By staying in the hotel or resort and taking advantage of the services in the resident bar or restaurant, the visitor minimizes contact with potential criminal elements. Furthermore, by charging
meals and drinks to the room, travelers avoid having to carry a large amount of cash.

Westerners who want to avoid danger while traveling abroad will arrive in their host country with a basic knowledge of local threats, laws and customs. Furthermore, they will avoid danger zones and maintain situational awareness — and exercise common sense — at all times.

Security During Adventure Travel

July 11, 2011

Over the course of this series, we have tried to prepare would-be travelers for some of the risks they may encounter while traveling abroad. This has led us to address a variety of forms of travel. However, another type of travel exists, one that we have yet to address, one that we believe distinguishes itself from other forms of travel and merits a closer assessment of the risks it presents: adventure travel.

Adventure travel involves traveling to remote locations and natural environments with little, if any, public infrastructure. Increasingly popular over the past 10 years or so, adventure travel typically involves a physical component, such as hiking or river rafting, and it has become an industry unto itself. All of the security suggestions and advice given in previous installments of this series are relevant to adventure travel, but this installment aims to highlight some of the issues a traveler should understand — and some of the risks a traveler should accept — before venturing into remote locales and undeveloped country.

Practice Adventure

Before going to a remote village in the mountains or embarking on a sailing trip around the world, a traveler must ask himself or herself if they really want adventure, or if they just want photographs of
adventure. There is a reason adventure travel destinations are sparsely populated: They are extremely difficult places to live. A critical safety precaution for an adventure traveler is to not take lightly or cavalierly the decision to travel.

Indeed, the best preparation for adventure is adventure closer to home. When planning a trip, a traveler should not plan a three-week climb to the base camp on Mt. Everest unless he or she has spent time in the mountains at high altitudes carrying 70 or more pounds on his or her back. It is advisable to become practiced at one’s adventure of choice, river rafting, for example, before making it the focus of a two-week trip to Costa Rica. A traveler should begin with small excursions — a day hike in places where there is no cell phone service — to experience what it feels like to be without water for up to six hours or to sleep outside when it is cold and rainy. These hardships will not endanger a traveler and will prepare him or her for the real thing.

An adventure traveler must be adaptable and accepting of hardship. The whole point of adventure travel is to abandon one’s comfort zone. Whether hiking through the jungle, kayaking down a river or staying in an indigenous community in the Andes, travelers are bound to encounter problems not easily solved — or problems that are impossible to solve. Buses may not arrive, guides will quit and the hostel might not even remotely resemble its online pictures. The biggest mistake a traveler can make in those situations is to spend too much time figuring out why something went wrong and not enough time figuring out how to resolve the situation. In an adventure situation, food, water and shelter are the only things that matter. Weather, while a consideration, is less of a concern if a traveler has appropriate shelter and the ability to protect himself or herself from the elements. All other considerations, such as a soft bed or a shower, should be considered luxuries.

Preparation, situational awareness and thoughtful action remain the foundation for mitigating risks in all forms of travel, but they become more important in adventure travel because, given the destinations, immediate support is difficult — if not impossible — to find.
In major cities of developing countries, an injured traveler can seek treatment at a hospital or clinic. A traveler who has lost his or her money can locate a bank to get more. If the hotel in which a traveler is staying is dangerous, there are other hotels in safer areas. Once outside of major cities, an adventure traveler’s options are more limited.

Plan Adventure

In the wilderness, the consequences for inadequate planning, lack of situational awareness or impulsive decisions can be death. In the event of an injury, very few options exist for a traveler, other than to stabilize the injury as much as possible and seek help. Planning is very important before going on an adventure trip, but planning a trip can be difficult in places of the world where little information is available. Travel guides, webpages and blogs can be valuable sources of information in such instances. However, adventure travel by its nature means less information will be available.

It is critical that a trusted friend or family member not going on the trip has a detailed itinerary and an emergency plan, including important phone numbers for the local consulate in a foreign country and the authorities, such as the local police, in developed countries. Because communication equipment can be nonexistent in some remotes destinations, travelers should decide prior to departure when they will return, designating a deadline after which their emergency contact will call the authorities.

Travelers should always leave a trail to be followed. They should sign and date as many guest books as possible at hostels and the front gates of parks or reserves or historical attractions they visit. They should also make allies and friends along the way with people who could remember them if shown a picture.

Another aspect of planning — and, thus, risk mitigation — is understanding what equipment is necessary for a specific location. Advances in technology have made adventure travel more accessible than ever. Water filtration devices, lightweight, easy to use white-gas stoves and clothing technology advancements have all made
adventure travel easier. However, travelers should never rely on technology to save them in an emergency. Lighters stop working, batteries run out and water filtration units break. Even satellite phones and other emergency response technology, while valuable, cannot always guarantee one’s safety.

Notably, preventable diseases in the developed world can be fatal in the wilderness and in the developing world requiring travelers to have a different mindset. They should be up to date on vaccines, especially hepatitis and tetanus. Doctors are sometimes willing to give travelers a few antibiotics or pain medications before they go to remote locations. Travelers should understand and be prepared for the indigenous flora and fauna, as well as for diseases that are specific to a location. Medical care in remote locations is sometimes non-existent, and having some training can sometimes save a life. Travel insurance that covers a traveler on adventure trips is also very important.

Threat recognition is paramount, and many travelers misread a situation because they do not understand the environment in which they find themselves. It becomes the responsibility of the traveler to have a plan in place in the case of emergency, to have proper training to know how to deal with the emergency and to make decisions after thoughtful consideration (if time allows).

Outdoor adventure schools such as National Outdoor Leadership School or Outward Bound can be great places to learn survival skills in the wilderness. These skills also translate to remote locations in third world countries and these schools allow novices to experience the wilderness while being trained in proper survival skills. At minimum, every adventure traveler should take a wilderness first aid course. Wilderness First Responder courses are highly recommended.

Many travelers are more comfortable going on pre-packaged trips with an adventure travel company rather than attempting to plan the trip themselves, especially if time is a factor. If a traveler chooses to go it alone, adaptability becomes all the more crucial because it is very difficult to make arrangements for nonexistent amenities. After all, one cannot plan a bus schedule where there are no buses, and one cannot make hotel reservations if there are no hotels. Pre-planned
trips, especially for one’s first time in a location, remove much of the stress involved in such scenarios. However, they also place limitations on the traveler — seemingly counterproductive for one seeking adventure in a foreign country.