ANTITERRORISM (AT) LEVEL I TRAINING

CENSECFOR-AT-010-1.0

Introduction

American's efforts to fight terrorism include virtually every government agency as well as friends and allies around the world.

Since September 11, 2001, the United States has been engaged in an effort to protect the nation's freedoms. The world is dangerous and we are at war against an enemy intent on destroying the American way of life. While responding to this real and present danger, we must remain vigilant while executing our responsibilities.

Stay alert, be aware of your surroundings, and report unusual or suspicious activity. Pay attention to the details of antiterrorism briefings you receive on your locale and when preparing to travel to a new location. Most importantly, make security a part of your routine. Exercise precautions to increase your personal security and the security of your family, colleagues, and organization.

Patience and persistence are the watchwords for defeating terrorists. They are patient and cunning, and they are waiting for you to let down your guard or settle into a pattern of predictable behavior. Do not be a tempting target. Be vigilant so we may successfully defend America and our freedoms.

Threat Factors

Improvised Explosive Devices (IEDs) may be disguised as everyday items.

There are eight factors you should consider to understand the threat in your environment. Using these factors, you can be better prepared for the potential risks you face.

1. Are terrorist groups in the area?
2. Are they violent?
3. Do they attack Americans?
4. How active are they?
5. How sophisticated are they?
6. Are they predictable
7. Will local citizens warn Americans?
8. What tactics and weapons are used?

Terrorism is the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religions, or ideological.

How Terrorists Identify & Select Targets

While overseas it is advisable to conceal your DOD affiliation.

Consider ways you might become a victim of a terrorist attack. Several factors to keep in mind include:

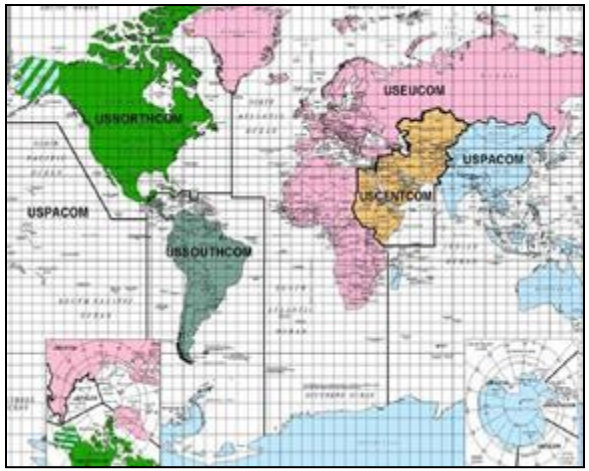
Location: Terrorists may target locations frequented by Americans or US military personnel such as certain hotels, apartment buildings, public transportation centers, and nightclubs. Avoid possible target locations.

Association: Terrorists may focus on American tourists, personnel associated with the US Government, and individuals who appear to be high-ranking or important. Try to blend in with the local population. When possible, avoid disclosing your DOD or US Government affiliation.

Opportunity: Terrorists look for "soft targets." Maintain vigilance, practice good personal safety, and alert the proper authorities of suspicious behavior.

To attack you, terrorists generally must perceive you, your association, or your location as a target. Do not be an easy target.

Combatant Command Overview



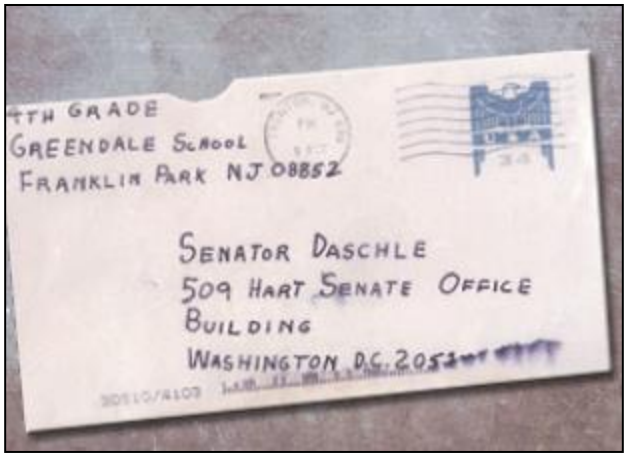
Threats vary in different parts of the world. Take time to learn about the specific threats in your area.

Groups and individuals have demonstrated their willingness to employ terrorist tactics to further their agendas. While some threats have a regional focus, others have become international and affect multiple areas. DOD personnel and assets have been targeted in virtually every region of the world.

When traveling, you should receive a Combatant Command terrorist threat briefing 90 days prior to departure. Modify your personal protective measures based upon the information in these briefings. Threat briefings are based upon intelligence and local historical factors and are designed to help you be safe – take them seriously.

The following is a brief overview of the terrorist threat by Combatant Command. More detailed information for your region is available through your local Antiterrorism Officer.

NORTHCOM Region



In 2001, anthrax tainted letters were sent to several prominent individuals, including the Senator Tom Daschle.

Within the United States, several organizations and individuals use terrorist tactics to achieve their goals. Other organizations provide direct and indirect assistance through fund-raising, recruiting, and training support.

Terrorist attacks by Islamic extremists began in 1993 with the first attack against the World Trade Center in New York. More recently, the foiled terrorist plot against Fort Dix, New Jersey demonstrates that Al-Qaida inspired groups still exist within the nation's borders.

Home-grown terrorism is also a reality. During the 1960s an d70s, the Weathermen and the Armed Forces for Puerto Rican National Liberation executed several small-scale terrorist attacks. More recently, violent elements include the anti-abortion Army of God, the eco-terrorist Earth Liberation Front, and other domestic anarchist groups and individuals. Homegrown terrorists have employed various tactics such as rudimentary letter bombs, improvised explosive devices, small arms attacks, and truck bombs. Bioterrorism is also a concern in view of the anthrax attacks in 2001.

Examples of prior terrorist activity in the NORTHCOM AOR include the Oklahoma City Bombing, Fort Dix Plot, and the 2001 Anthrax Attacks.

CENTCOM Region

Terrorists used a VBIED to attack Khobar Towers in 1996

Within the CENTCOM region, Islamic extremists pose the primary terrorist threat to US military and government personnel. Since the mid-1990s, terrorists have enhanced their capabilities and expanded their influence and presence into other parts of the world.

In the areas of current US military operations, roadside Improvised Explosive Devices (IEDs) pose one of the greatest threats to US forces. Additionally, local political leaders, civilians, infrastructure, and international aid personnel are terrorized by suicide bombings, kidnappings, and murders. In many other parts of the CENTCOM region, suicide bombers and gunmen target hotels and tourist attractions to advance domestic political and religious agendas.

Numerous terrorist organizations operate within the CENTCOM region. In addition to Al-Qaida, other organizations include Hezbollah, the Palestinian Islamic Jihad, and the Ansar al-Islam.

Examples of prior terrorist activity in the CONTCOM AOR include the Serena Hotel, Luxor Massacre at Deir el0Bahri, and Khobar Towers.

PACOM Region

In 2008, terrorists attacked multiple targets in Mumbai, India including the Taj Mahal Hotel.

Terrorist groups in the PACOM region present diverse threats to Americans. Some specifically target Americans and others target public sites where Americans may become victims. Additionally, there is evidence of ties between groups in the PACOM region and al Qaida and other international groups.

Terrorist attacks in this region demonstrate a broad spectrum of tactics. These include kidnappings, suicide bombings, and even chemical attacks. Aleph, formerly known as Aum Shinrikyo, attacked the Tokyo subway with Sarin nerve gas and cyanide in 1995. Abu Sayyaf, a Philippine group seeking to create a radical Muslim state, targets Americans for kidnapping.

Terrorists have targeted DOD and other American assets in the region. In 2001, Singaporean officials foiled a plot to attack US military forces and western diplomatic missions. The group, Jamaah Islamiya, seeks to create a radical Muslim state across South East Asia. In 2002, 2005, and 2009 it conducted bombings in Bali and Jakarta, Indonesia to kill western tourists.

Examples of prior terrorist activity in the PACOM AOR include the Mumbai Attacks, the Singapore Plot, and Tokyo Subway Attack.

SOUTHCOM Region

Narcoterrorism, as demonstrated by the August 2011 attack against the Casino Royale in Mexico, is a growing concern for US officials.

The primary terrorist threat in the SOUTHCOM region is narcoterrorism and the continued operation of radical leftist groups. Additionally, the ties between narco-terrorists and radical extremists from the Middle East are reportedly increasing. It is possible Latin American countries may become a transit point for terrorists from other parts of the world to enter the United States.

Unlike the 1980s, recent attacks against US interests are focused primarily on businesses and not US military or government assets. In addition to bombings and arson, terrorist tactics include targeted assassinations and kidnapping, especially against non-US assets.

Some of the most prominent terrorist organizations within the SOUTHCOM region include the Revolutionary Armed Forces of Colombia (FARC), the Colombian National Liberation Army (ELN), and the Shining Path in Peru.

Examples of prior terrorist activity in the SOUTHCOM AOR include the Attack on the Japanese Ambassador's Residence in Peru, Zona Rosa, and Casino Royale.

Terrorist Planning Cycle Overview

Learn the terrorist planning cycle so you will be in position to identify early indications of a potential threat.

Terrorist prepare and conduct attacks through predictable steps. Through vigilance, you may be able to recognize preparations for an attack before it is executed.

Be alert to unusual behavior that may indicate intelligence gathering, surveillance, collecting materials for attack, dry runs, and rehearsals. For example:

- Taking Photos or videos of potential targets
- Writing notes or sketching details about a possible target
- Showing abnormal attention to details of routine activities and security measures
- Using false identification
- Paying cash for items normally bought on credit
- Purchasing large quantities of items that could be used as part of an attack (e.g., chemicals or cell phones).

If you see something unusual, report it immediately to security officials for further investigation. Make a note of the individual's description and activities, the time of day, and equipment being used.

On the following screens, the planning and execution of the attack on the Murrah Federal Building in Oklahoma City illustrates this process. Consider how a vigilant person might have recognized indications of a threat.

Terrorist Planning Cycle – Phases 1 & 2

Timothy McVeigh targeted the Murrah Federal Building because of the presence of US Government agencies.

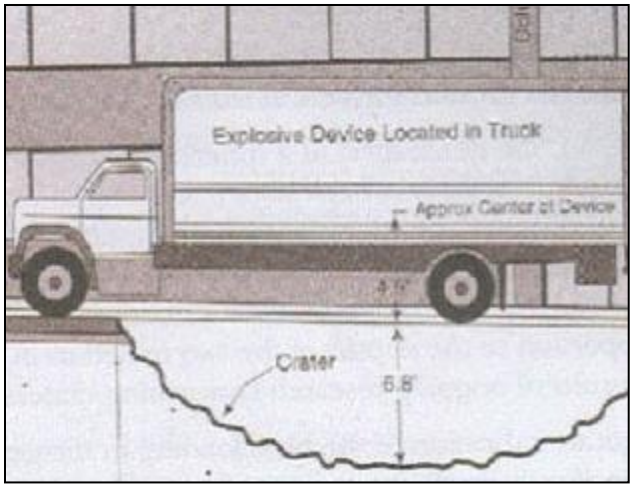
Phase 1: Broad Target Selection. During broad target selection, terrorists collect information on numerous targets to evaluate their potential in terms of symbolic value, casualties, infrastructure, criticality, or public attention.

Timothy McVeigh wanted to attack a symbol of the federal government, preferably the FBO, Drug Enforcement Administration, or Bureau of Alcohol, Tobacco and Firearms. He identified possible targets such as individual federal employees, their families, and facilities in at least five states.

Phase 2: Intelligence and Surveillance. Vulnerable targets able to meet attack objectives are selected for additional intelligence gathering and surveillance. This effort may occur quickly or over years depending upon the target and planning information needed. Terrorists seek to gather detailed information on guard forces, physical layout, personnel routines, and standard operating procedures.

McVeigh performed initial surveillance on the Murrah Federal Building in Oklahoma City, one of his potential targets. He noted the interstate highway allowed easy access and possible escape routes. He also observed indented curbs that permitted vehicles to be parked directly in front of the building.

Terrorist Planning Cycle – Phases 3 &4



The placement of the vehicle bomb outside the Murrah Federal Building and the resulting crater from the explosion.

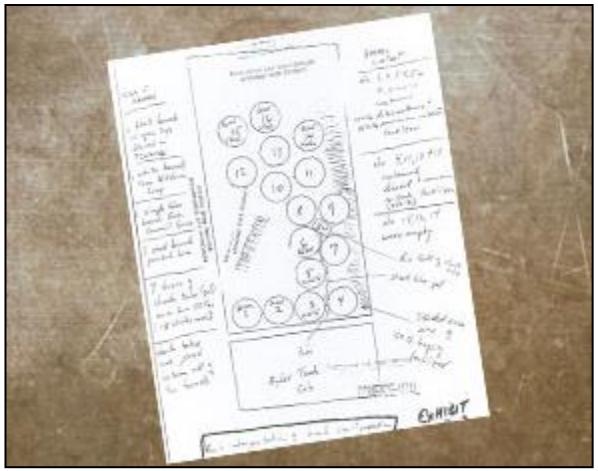
Phase 3: Specific Target Selection. Specific targets are then identified for attack based on anticipated effects, publicity, consistency with overall objectives, and costs versus benefits of the attack.

McVeigh chose the Murrah Federal Building because he believed the Federal agencies represented there were responsible for the incident in Waco, TX two years earlier. In addition, he assessed the facility as a "soft target," with a good chance of success at low risk. His intent was to kill Federal employees and thereby gain media attention.

Phase 4: Pre-Attack Surveillance and Planning. Terrorists may conduct additional surveillance to confirm previous information and gain additional details. During this stage, terrorists will select the method of attack, obtain weapons and equipment, recruit specialized operatives, and design escape routes.

McVeigh recruited Terry Nichols and prepared for the Oklahoma City attack over a six-month period. He acquired materials for a 5,000 pound truck bomb through theft, use of false documents, and paying cash for items normally bought on credit. He also made several trips to the Murrah Federal Building to identify the exact place to park the truck and to select escape routes.

Terrorist Planning Cycle – Phases 5&6



A diagram drawn by McVeigh showing the configuration of the vehicle bomb.

Phase 5: Rehearsals. Terrorists often rehearse the attack scenario to confirm planning assumptions, enhance tactics, and practice escape routes. They may also trigger an incident at the target site to test the reaction of security personnel and first responders.

McVeigh practiced making an detonating bombs in isolated locations. He memorized details of the Murrah Building layout, finalized the sequence of actions for the attack, and practiced responses to law enforcement officers if they were encountered.

Phase 6: Actions on the Objective. Terrorists choose to execute attacks when conditions favor success with the lowest risk. Factors they consider include surprise, choice of time and place, use of diversionary tactics, and ways to impede response measures.

On 19 April 1995, McVeigh parked a rental truck – a 5,000 pound vehicle bomb – in front of the Murrah Federal Building where it could cause the most damage. The date of the bombing was symbolic – the second anniversary of the fire at the Branch Davidian compound in Waco, TX.

Terrorist Planning Cycle – Phase 7

McVeigh's getaway car after his arrest.

Phase 7: Escape & Exploitation. Unless an operation is a suicide attack, escape routes are carefully planned and rehearsed. Terrorists may exploit successful attacks by releasing pre-developed statements to the press.

After preparing the bomb for detonation, McVeigh walked away from the scene on a preselected route. To flee Oklahoma City, McVeigh used a get-away car pre-positioned before the attack.

McVeigh wanted to world to know that he attacked the Federal Murrah Building because he believed the Federal Government infringed on individual rights of Americans. McVeigh left a file on his sister's computer titled "ATF Read" echoing these sentiments. His get-away car contained anti-government literature and he subsequently made statements concerning his motivations for the attack.

FPCONs

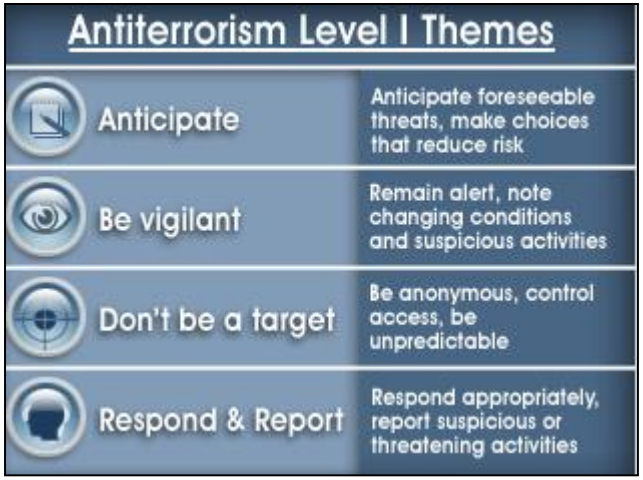
Terrorists used a VBIED to attack Rhein-Main Air Base in 1985

US Military facilities use a variety of protective measures to reduce vulnerability to terrorist attack. These measures are organized in a system called Force Protection Conditions, or FPCONs. As the threat changes, Commanders change the FPCON to protect personnel.

FPCONs are organized in five levels with increasing measure of protection: NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA. Commanders adapt protective measures for the local situation, and they can use additional measures and move to a higher FPCON as needed. Measures may also be added randomly to rehearse them, to promote security awareness, and to confuse surveillance by potential threat elements.

As the FPCON increases, you can expect to experience delays at gate checks, more detailed inspections, gate closures, and increased guard presence. FPCON CHARLIE and DELTA are very restrictive and rarely used. Normal operations may be reduced or suspended in these cases.

AT Fundamentals Introduction



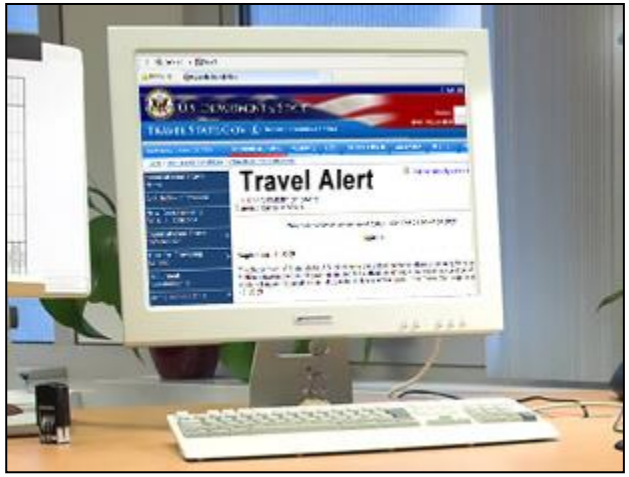
The four AT Level I themes: Anticipate, Be Vigilant, Don't be a Target, and Respond and Report.

The next section of this training will introduce you to AT security in several different environments. These are presented in the following groups:

- Surveillance detection
- Security at a government facility
- Residential security
- Security during off-duty/free time activities
- Air travel security
- Ground travel security
- Hotel security
- Hostage Survival
- CBRNE

The next several screens introduce the four antiterrorism themes found throughout the training.

Anticipate



Even if you receive official security briefings, there are several sources that allow you to research threats for yourself.

Anticipating threats, risks, and vulnerabilities is key to antiterrorism security and personal protection.

Research prior terrorist attacks to understand the tactics used by local terrorists and the types of targets they have attacked. Consider consulting these sources of information:

- Embassy Regional Security Office
- State Department Travel Warnings
- Other internet & media resources

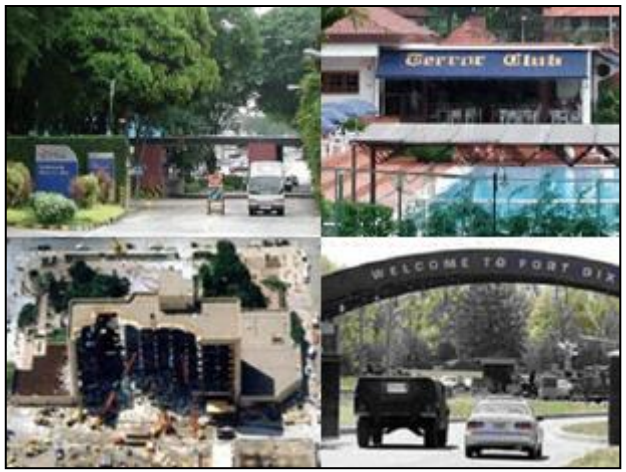
Consult the Foreign Clearance Guide and comply with specific requirements for security and coordination. Also, get a threat briefing before departing or upon arriving at your location.

These will help you:

- Determine places you should and should not visit
- Identify appropriate security measures
- Recognize and respond to possible threats
- Make personal security and emergency plans

Planning ahead can enhance security in your travels.

Be Vigilant



Many terrorist attacks can be thwarted through the recognition of pre-attack surveillance activities

Vigilance is required to continuously observe your surroundings and recognize suspicious activities.

The first step to vigilance is to understand your environment's normal conditions. To do this, try to observe and learn the patterns of routine activities in your area.

When you have an instinct for what is normal, you can recognize things that are suspicious:

- Potential threats such as items that are out of place
- Attempted surveillance by persons who are loitering, following you, or simply in the wrong place
- The presence of circumstances that correspond to prior attacks in your area

Informed vigilance is fundamental to personal security and may allow you to identify, report, and thwart a potential threat.

Don't be a Target

Items that display your DOD affiliation may also help identify you as a potential target.

Not all threats are predictable or can be recognized in advance. As a result, you should concentrate on not being an easy target for a terrorist attack.

Reduce your exposure by being anonymous and blending in with your surroundings

- Do not wear clothing or carry items that identify your DOD affiliation
- Remain low key and do not draw attention to yourself
- Avoid places where Americans are known to congregate

In addition to blending in, try to reduce your vulnerability and exposure:

- Select places with security measures appropriate for the local threat
- Be unpredictable and vary your routes and times of travel
- Travel with a friend or in a small group
- Use automobiles and residences with adequate security features

You can greatly increase your personal protection posture by remaining anonymous and reducing your exposure.

Report & Respond

The Fort Dix attack plot was thwarted by a store clerk that recognized suspicious circumstances and reported them to the FBI.

Report suspicious activities to appropriate authorities immediately. And, when threatened, respond to protect yourself and others. Specific circumstances may require different responses; however, in general:

- Report suspicious activity, do not try to deal with it yourself
- In threatening situations, take steps to reduce your exposure
- Follow the instructions of emergency personnel and first responders

Security is a team effort. Try to ensure your actions help trained security personnel do their jobs. You can do this by providing information they need and avoiding becoming a casualty yourself.

Upon arrival at a new location, learn the proper procedures for reporting antiterrorism related information. This could be a unit antiterrorism officer, a US Embassy security officer, or local law enforcement. Be prepared to report and respond.

Surveillance Detection Introduction

Terrorists conducted an extensive surveillance against the US Air Force installation in Sembawang, Singapore. An operative narrated a video while walking around the installation with a camcorder.

Terrorists conduct surveillance to gather information to plan an attack. Criminals perform surveillance to choose a time and place to conduct a theft. In both cases, the target of surveillance may be an individual, a facility, or asset.

Surveillance against an individual seeks to determine:

- Residential security measures
- Modes of travel
- Routes and times of travel
- Typical behavior
- The target's general security awareness

Surveillance against a facility or asset tries to determine:

- General security posture
- Security standard operating procedures
- Information on security force shift rotations
- Physical security weaknesses
- Reaction times to emergencies

Detecting terrorist surveillance is key to preempting a terrorist attack. If you detect possible surveillance, contact unit or installation immediately.

Surveillance Detection Fundamentals

Terrorists performed extensive surveillance of the Terror Club in Singapore with a handheld camcorder. The activity was not detected or reported.

Be alert to the possibility of surveillance on-and off-base. To recognize suspicious behavior, try to:

- Get to know your neighbors
- Learn to recognize legitimate vehicle and uniform markings of utility workers and local law enforcement
- Understand the pattern of routine activities on your installation and in off-base areas you frequent
- Learn the local culture

In conducting surveillance, terrorists try to blend in with the environment to avoid arousing suspicion. Be alert for anythign that might be a sign of surveillance:

- People remaining in or coming back to the same general area without a recognizable reason
- People preoccupied with a specific area, to include taking pictures, making notes, or drawing sketches
- Certain civilian vehicles that seem to appear repeatedly
- Utility and constructions workers that do not appear to be performing a specific job
- Electronic audio and video devices in unusual places or that are not DOD property

Learn your environment and recognize suspicious behavior!

Methods of Surveillance 1

Surveillance may be conducted over a long period of time and employ various methods:

Stationary surveillance: operatives observe from a fixed location

- Operatives try to blend in by doing ordinary tasks
- Operatives may seek to recruit host nation support personnel or domestic help with access to installations or residences

Moving surveillance: conducted on foot or in vehicles, generally in teams.

- Vehicle surveillance may include one or more vehicles
- Generally uses two or more people, one driving while the others observe
- Operatives may not always be behind you; once your routines are learned, they may be in front of you

Varying your routes and routines can disrupt surveillance attempts.

Methods of Surveillance 2

Many everyday items can be used for surveillance activities

Additional surveillance methods include:

Technical surveillance: uses electronic means to record or gain access to security information.

- May use still and video cameras, including cell phones
- May gain access to security information on the Internet

Casual questioning: used to elicit security information from approachable personnel.

- Operatives may portray themselves as non-threatening and friendly
- Terrorists may use unwitting operatives who do not understand the purpose of the informaiton they are asked to gather
- Operatives may use members of the opposite sex to gain access to facilities and collect information

Awareness of terrorist surveillance methods can help you see and respond to surveillance.

Surveillance Detection Situation 1

The Fort Dix Six used a pizza delivery service to gain access and perform surveillance of Fort Dix

You are stationed overseas and have been provided on-base housing.

One day as you come out of your house you notice a delivery van belonging to one of the local vendors that works on your installation. It is parked a couple of houses down and a single individual is sitting in the driver's seat looking around.

There is no real reason why a vendor vehicle should be in the residential section of your base.

You know you should note the driver's description. But what else should you do? (Choose one!)

1. Wait until the vehilcle leaves and follow it
2. Continue to observe the vehicle to collect as much information as possible
3. Note the vehicle make, model, and license plate number and immediately report to unit or installation security

Surveillance Detection Situation 1- Answer

The Fort Dix Six used a pizza delivery service to gain access and perform surveillance of Fort Dix

You are stationed overseas and have been provided on-base housing.

One day as you come out of your house you notice a delivery van belonging to one of the local vendors that works on your installation. It is parked a couple of houses down and a single individual is sitting in the driver's seat looking around.

There is no real reason why a vendor vehicle should be in the residential section of your base.

You know you should note the driver's description. But what else should you do? (Choose one!)

1. Wait until the vehilcle leaves and follow it
2. Continue to observe the vehicle to collect as much information as possible
3. **Note the vehicle make, model, and license plate number and immediately report to unit or installation security**

Government Facility Security Fundamentals

Be a team player; cooperate with installation security procedures.

The success of installation security protocols and procedures depends on their consistent application. This requires discipline, attention, and cooperation from everyone.

By understanding security at your installation, you may see something that dedicated security personnel are not able to see, or you may see a problem that is not obvious to others.

- Be aware of the current Force Protection Condition (FPCON) and comply with security and response protocols
- Understand the features of your installation's security system
- Recognize non-malicious compromises in security
- Recognize potentially malicious threats to security
- Report lapses in security or suspicious behavior
- Know what to do in response to an incident
- Understand your responsibility if you are detailed to support security tasks.

Installation security is a team effort and everyone has a security responsibility.

Recognizing Problems in Government Facility Security

Report suspicious behavior to the appropriate personnel.

Every individual can play an important role in identifying and reporting problems in security.

Security may be weakened in an unintentional manner through a lack of discipline. Or, low-level behaviors may suggest a malicious intent. Report problems you observe:

- Inattentive guard personnel
- Weapons, identification badges, or keys managed in a non-secure manner
- Gaps in procedures that leave unauthorized persons unsupervised in sensitive areas
- Persons with an inappropriate curiosity in security measures
- Persons attempting to photograph security measures
- Persons attempting to conceal contents of bags or cargo

Do not assume that dedicated security personnel can see everything. You are the eyes and ears that complete the security picture.

Government Facility Incident Response

Be familiar with emergency response procedures so you can react appropriately.

Every DOD member needs to be informed and ready to respond appropriately to incidents on the installation.

Consider the following:

- Be aware of emergency contact phone numbers and procedures
- Be familiar with the location and use of fire fighting equipment and first aid kits
- Know and rehearse evacuation and accountability procedures for work places, quarters, and other frequently used facilities
- Be aware of normal patterns of activities and respond quickly to things that are unusual

Each individual's response should seek to secure their personal safety, protection of other persons, and preservation of DOD property.

Emergency response requires preparation and decisive action.

Government Facility Security Situation

Observe and learn the security protocols of your installation and help others do the same.

You are newly assigned to a US installation in a region without much history of terrorist activity against US and allied interests.

You know to ask for an orientation briefing on threats in your new area of operation and an orientation on security procedures. What else can you do to become a better team member on security matters? (Choose one)

1. Ask relatives back home to send general information on the history of the region
2. Learn the normal routines of the installation so you can recognize suspicious behavior
3. Try to learn enough of the local language to pick up news from local sources

Government Facility Security Situation - Answer

Observe and learn the security protocols of your installation and help others do the same.

You are newly assigned to a US installation in a region without much history of terrorist activity against US and allied interests.

You know to ask for an orientation briefing on threats in your new area of operation and an orientation on security procedures. What else can you do to become a better team member on security matters? (Choose one)

1. Ask relatives back home to send general information on the history of the region
2. **Learn the normal routines of the installation so you can recognize suspicious behavior**
3. Try to learn enough of the local language to pick up news from local sources

Insider Threat Introduction

Suicide belts and other IEDs are common weapons against US forces in deployed areas.

An Insider Threat uses authorized access, wittingly or unwittingly, to harm national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.

Examples of attacks allegedly perpetrated by individuals thought to be loyal to the US include:

- 2010 leaking of over 500,000 documents concerning operations in Iraq & Afghanistan
- 2009 Active Shooter attack at Fort Hood
- 2003 Active Shooter attack at Camp Pennsylvania
- 2001 anthrax attacks against government facilities; perpetrator possibly associated with USG

Motivations for the insider threat may include:

- Desire to further a political or religious agenda
- Ability to exert power to influence events
- Perceived injustices upon oneself or against a minority group
- The need for excitement
- The desire to commit suicide

Individual awareness and active leadership are key defenses to the Insider threat.

Types of Insider Threats

In October, 2010, the National Museum of the Marine Corps was targeted by a drive by shooter

Types of Insider Threats related to antiterrorism include:

Terrorism Intended to Coerce or Intimidate: Persons who plot and execute attacks to further the agenda of an extreme ideology

Mental Instability: Persons that have a mental illness that impairs their judgment.

Espionage: The divulgence of classified or sensitive information that may result in attacks or provide information on vulnerabilities that facilitate an attack. Motivations may be financial or ideological.

Negligence: The disregard for standard security measures that potentially allow the collection of vulnerability-related information or information that could precipitate an attack.

Preconditions for the Insider Threat may include:

- An opportunity to commit the act
- A motive or need to be satisfied through the act
- An ability to overcome natural inhibitions to criminal or violent behavior
- A trigger that sets activities in motion

Security personnel cannot recognize and defeat all threats. You must be vigilant to a variety of potential threats.

Recognizing Political/Religious Extremism

Humam Khalil Abu-Mulal al-Balawi detonated a suicide bomb at Camp Chapman in Afghanistan killing seven CIA operatives.

Early recognition of an Insider Threat can prevent an incident. Pre-attack indicators of terrorism intended to coerce or to intimidate mostly in pursuit of ideological, religious, or politicial reasons include:

- Anti-American statements that US policy and authority is illegitimate
- Aggression or threats toward coworkers
- Presence of unauthorized weapons
- Attempts to communicate with US enemies
- Associations with known extremist groups
- Distribution of propaganda materials in support of an extremist position
- Unfounded allegations of US persecution or prejudice against a minority group or religion
- Repeated violation of policies

If you perceive an immediate violent threat, alert security personnel or law enforcement personnel immediately.

Recognizing Political/Religious Extremism

Abuse of alcohol and drugs is a possible indicator of the insider threat.

A mentally unstable person may or may not exhibit some of the same behaviors of a prospective terrorist. Indicators of a potentially unstable person often include:

- Abnormal mood swings or depression, withdrawn behavior, decrease in hygiene, and paranoia
- Flashbacks to prior tramautic events
- Abuse of alcohol or drugs
- Repeated violation of policies
- Talk of domestic or financial problems
- Talk of suicide
- Intense anxiety in social situations

If you witness behavior that might indicate an unstable person, you should alert your supervisor or appropriate medical personnel immediately. Early detection of such behavior can prevent a violent incident and help a person get the help they need.

Active Shooter Introduction

In October 2002, over 40 heavily armed Chechen rebels attacked and held hostage occupants of the Dubrovka Theater in Moscow, Russia

An active shooter incident can occur at any time and at almost any location. Recent examples of active shooter incidents include:

- March 2011 shooting of Air Force personnel at Frankfurt Airport in Germany
- November 2009 shooting at the Soldier Readiness Center in Fort Hood, Texas
- June 2009 shooting at Holocaust Museum in Washington, D.C.
- May 2009 shooting of soldiers outside a military recruitment center in Arkansas
- November 2008 attacks against hotels, restaurants, and a train station in Mumbai, India

It is unlikely you will be involved in an Active Shooter incident, but you should be prepared for the possibility.

Active Shooter Fundamentals

If you are in an exposed position, try to seek cover in a room or place that can be sealed off or barricaded.

Active shooter situations are unpredictable and can evolve quickly. Potential responses include:

- Evacuate
- Shelter in place
- Take action against the perpetrator
- Cooperate with first responders

You can also adapt your response to the type of weapon used by an attacker:

- Ricocheting bullets tend to hug the floor; crouching (not lying) on the floor may reduce exposure
- Grenade shrapnel rises from the detonation; lying on the floor reduces exposure and having feet toward the blast may protect the head

An active shooter situation may be over within 15 minutes, before law enforcement arrives. Be mentally and physically prepared to deal with an active shooter situation.

Responding to an Active Shooter

In an active shooter situation, evacuate if possible.

If you are in the vicinity of an active shooter situation, you have several options for response.

Evacuate. If there is an escape path, attempt to evacuate. Be sure to:

- Have an escape route and plan in mind
- Evacuate regardless of whether others follow
- Leave your belongings behind
- Help others escape, if possible
- Prevent others from entering an area where the active shooter may be
- Keep your hands visible
- Follow the instructions of first responders
- Do not attempt to move wounded people
- Call emergency services when you are safe

Evacuations may not always be possible and you may need to consider other options.

Responding to an Active Shooter 2

If necessary, you should be prepared to shelter in place.

If evacuation is not possible, consider the following.

Shelter in place: Find a place where the active shooter is less likely to find you. Remember to silence your cell phone, remain quiet and calm, and call emergency personnel if possible.

The place you choose should:

- Be out of the shooter's view
- Provide protection against shots fired your way
- Not trap you
- Have locks on the door
- Have furniture to blockade the door

Take action against the active shooter: As a last resort, and only when your life is in imminent danger, try to disrupt or incapacitate the shooter by:

- Acting aggressively
- Throwing items and improvising weapons
- Yelling
- Committing to your actions

Taking action against the active shooter may be risky, but it may be your best chance for survival.

Arrival of First Responders

Two Air Force personnel were killed and two wounded at an Active Shooter incident at Frankfurt International Airport in March 2011

When first responders arrive, support their efforts and do not be a distraction:

- Remain calm and follow instructions
- Put down any items in your hands
- Raise hands and spread fingers
- Keep hands visible at all times
- Avoid quick movements
- Do not cling to emergency personnel
- Do not stop to ask first responders for help or direction when evacuating
- Evacuate in the direction first responders are entering

Provide first responders with the following information:

- Location and number of perpetrators
- Number of shooters
- Physical description of shooter(s)
- Number and type of weapons held by the shooter(s)
- Number of potential victims

It is normal to feel helpless; however, you can support first responder efforts.

Residential Security Introduction

Each type of residence has its own security strengths and vulnerabilities. Consider the local threat when selecting your home.

Living overseas can be an adventure. Good security can increase your confidence and make it more enjoyable.

You may have limited choice in selecting your residence. DOD members live in US military installations, DOD-leased apartments, residences pre-approved by the US Embassy or US Command, or residences of their own choice.

Terrorist attack on a private residence is less likely than theft or home invasion. But, crime prevention measures will also enhance your antiterrorism posture.

Follow the guidance of your housing authority. Some considerations include:

- Location in a low crime area
- Access to US facilities and local emergency services
- Security measures such as apartment visitor/vendor control and gated-community access controls
- Strong crime prevention measures

A concentration of American residences could be a target for crime or terrorism. But, an isolated location may be a target for criminal break-in.

Residential Security – Physical Security

When in a new home, you do not have to settle for security measures in place. There are many things you can do to enhance your home's security.

Look at your residence the way a criminal might. Physical security measures are a deterrent against crime.

Consider these measures:

- Check for solid exterior doors, good locks, deadbolts, slide locks, and reinforcing plates to protect locks and door jams
- Ensure sliding doors cannot be lifted from their track and lay a rod or dowel in the track
- Keep valuables out of sight and away from exterior windows
- Do not hide spare keys outside
- Do not advertise your name, rank, or nationality
- Use an alarm system when you are at home and away
- Improve exterior lighting
- Put gravel outside windows so a prowler will make sound

Consider replacing locks since you do not know who may have keys from previous tenants.

A home that is an easy target is also a more likely target.

Social Media

Information posted on social media sites should be reviewed for OPSEC considerations.

Social media provides many advantages. However, through social media, users can inadvertently provide information on:

- A current operational mission
- An installation's mission and infrastructure
- Your schedule and routines
- The identities and activities of family member
- Aspects of lifestyle that could allow blackmail/coercion

To reduce the chances of inadvertently releasing sensitive information consider the following:

- Limit profile information and do not provide your job title, address, phone number, family member information, etc.
- Limit "friending" to people you know; consider verifying that other users' profiles are who they appear to be
- Limit information viewable by users not in your networks
- Use high profile security settings and disable GPS tracking and facial recognition options
- Never post information or photos that describe current duties or operational locations
- Monitor internet usage of family members
- Report suspicious inquiries or violations of internet usage

Social media is an advantageous tool, but information provided over the internet can potentially be used to plan and execute an attack against yourself, your family, or your unit.

Residential Preparation for Emergencies

Emergency preparedness kits can benefit you during a security incident or natural disaster.

Be prepared to spend 72-hours in your home in an emergency. Make an emergency kit with food, bottled water, and first aid supplies. You can get an emergency kit checklist and a draft family emergency plan on-line.

Consider what to do in the following situations:

- A utility worker says he needs to check a gas line in your house…
  - Call the utility company to confirm identity and authority to enter
- Your children come home from school and unexpectedly no one is there to care for them…
  - Have an emergency contact plan and instructions to stay in a safe place
- Someone breaks into your home and demands money and valuables
  - Cooperation is probably the best approach

Discuss these and other contingencies to ensure your entire family is ready for the unexpected.

Off-Duty Security Introduction

Piccadilly Circus in London is a popular shopping and theater district. British authorities thwarted a terrorist attack against this cultural site in 2007

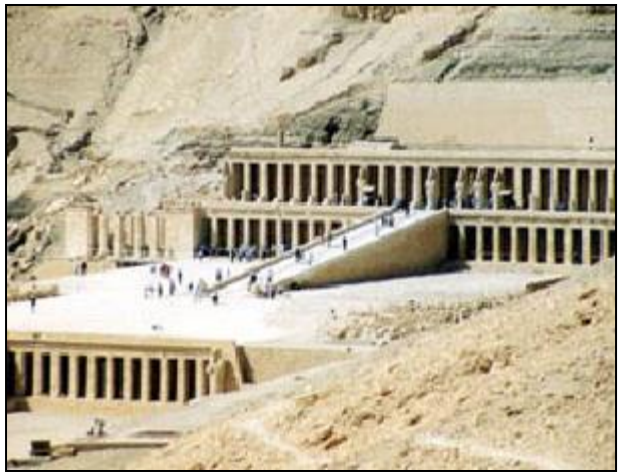
Off-duty time present opportunities to visit cultural sites or other civilian establishments. In some environments, terrorists attack these sites because they are vulnerable targets with an exposed population.

Keep risks in mind as you consider visiting civilian facilities like these in your off-duty hours:

- Places of worship and religious events
- Common tourist attractions
- International hotels
- Restaurants and coffee shops
- Night clubs
- Public transportation hubs
- Sporting events

Outside the protection of your installation or residence, your vulnerability may be increased. Consider your personal security during off-duty activities.

Off-Duty Fundamentals



Using automatic weapons and knives, terrorists attacked tourists at the Temple of Hatshepsut in Deir el Bahri, Egypt killing 62.

Several basic measures can enhance your security during off-duty activities. These include:

- Travel in a small group
- Do not draw attention to yourself; instead, conceal your military affiliation and try to blend in
- Carry emergency phone numbers
- Let someone else know where you are going.

Also, it is good to avoid:

- Places where Americans and other Westerners are known to congregate
- Places of religious significance
- Political events
- Going out on holidays or anniversaries that may temporarily increase the local threat

Follow any specific guidance from your unit or the US Embassy's Regional Security Officer.

Public Transportation

Public Transportation may be an option for getting to off-duty activities. If so, consider these protective measures:

- Select major hubs that might have better security
- Do not wait in large groups
- Change times and routes for places you visit often
- On an overnight bus or train, take food or drink only from official transit personnel
- In a train sleeper car, lock the compartment door securely and keep an exterior window cracked – criminals have used gas to knock victims unconscious

If taxis are used, consider these guidelines:

- Look for legitimate company markings on the taxi
- If a license is viewable, match the photo on the license to the driver
- Do not always use the same taxi company
- Select your own taxi, do not let a stranger select it for you

Public transportation in foreign countries can be confusing, intimidating, and dangerous. But you can take steps to reduce your vulnerability.

During Your Activity

The four bombers responsible for the 2005 attack against the London subway system entering Luton train station on the morning of 7 July 2005.

While visiting civilian sites for off-duty activities, there are several actions you can take to reduce your risk. These include:

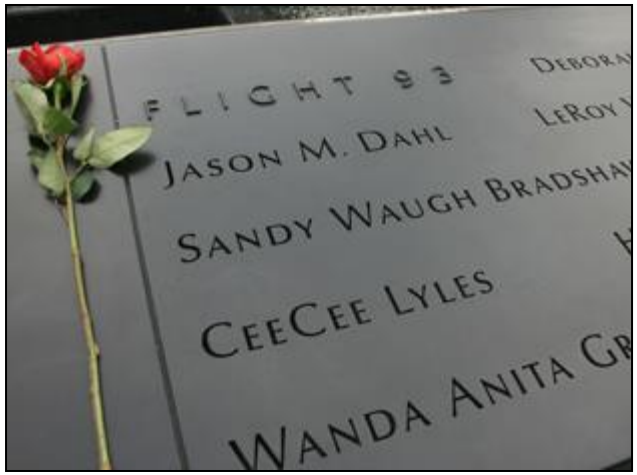
- Identify exit routes to be used in case of an attack
- Pre-designate a location to meet if your party is separated in an emergency
- Watch for suspicious behavior in others
- Notice objects that might conceal an improvised explosive device such as abandoned backpacks or unusual items in trash receptacles

In the event of an attack, remember the following:

- In a grenade attack shrapnel will rise from a point of detonation; being on the floor reduces exposure and having feet toward the blast may protect the head
- In a small arms attack ricocheting bullets tend to hug the floor; crouching (not lying) on the floor may reduce exposure

Enjoy your off-duty activities, but remember there is a threat. If you observe any indications of a threat, leave the area immediately and alert the appropriate US or local authorities.

Air Travel Introduction



The Flight 93 Memorial in New York honors those who died in an effort to wrestle control of their airplane from terrorists on 11 September 2001.

The attacks of 11 September 2001 demonstrated the threat terrorism poses to air travelers. Since then, security at airports and aboard aircraft has been increased.

However, even with increased security, the threat remains. Consider the following tactics and examples since 2001:

- Midair explosion - December 2001 shoe-bomb plot on a trans-Atlantic flight
- Surface to air attack – 2002 shoulder-fired missile attack on a civilian aircraft in Mombasa, Kenya
- Small arms attacks – 2002 attack against the El Al ticket counter in Los Angeles
- VBIED – 2007 attack against the Glasgow International Airport terminal
- Attacks against airport infrastructure – 2007 plot against John F. Kennedy airport
- Skyjacking – several incidents in Africa and the eastern Mediterranean

Some tactics against air travelers can be thwarted through vigilance. If you see suspicious behavior, report it to airport security personnel immediately.

Air Travel Fundamentals

Items that show your DOD or Government affiliation should be concealed.

Everyone should seek and receive guidance before traveling internationally. Some suggestions here may or may not be relevant to your specific travel situation.

It is generally wise to keep a low profile and not disclose your DOD affiliation:

- Travel with a tourist passport (consult Foreign Clearance Guide)
- Do not wear clothing with DOD or US symbols or slogans (check with your organization about clothing guidelines)
- Do not include rank or organization on luggage tags
- Use civilian luggage instead of military duffle bag
- Seal official papers in an envelope

When planning your travel, consider the following:

- Travel on US carriers or only on foreign carriers known to have good security
- Avoid airports with a history of security problems such as Athens and Istanbul

Consider your seat selection. A window seat reduces your exposure in a skyjacking but also reduces your mobility.

You can reduce risk with careful air travel planning.

Airport Terminal Security

A vehicle catches fire after terrorists ram the terminal building at Glasgow International Airport.

Threats against air travelers occur primarily in two places: at the airport prior to passing security and on the aircraft.

When you arrive at an airport, pass through security without delay since all passengers and baggage are screened at that point. To avoid delays, ensure your travel documents are in order and use online check-in options.

Be vigilant for:

- Vehicles left unattended at the curbside check-in areas
- Individuals that appear nervous
- Any activity that is out of place in an airport environment

Report suspicious activity to airport authorities immediately. In international or unfamiliar airports, it is best to wait for your flight in the gate area.

Responding to a Skyjacking

Threats to an aircraft come in many forms, and each terrorist may have a different motivation.

11 September 2001 introduced a new tactic to airline skyjacking: use of aircraft as weapons of mass destruction. However, skyjacking is still used to take hostages and not all skyjackers are intent on suicide.

If your aircraft is skyjacked, you must choose your actions carefully whether to cooperate or actively resist. Try to understand the skyjackers' intent. For example:

- Are pilots left in control of the aircraft? This may indicate a desire to land the plane safely
- Have passengers or crew been physically abused? This may indicate their mindset
- Are passengers singled out by nationality or religion? This may indicate something about their goal

More information about responding to a hostage situation is available in the Hostage Survival section of this application.

Ground Travel Introduction

Terrorists used hand guns to assassinate Lieutenant Commander Albert Shaufelberger in El Salvador and Captain George Tsantes in Greece. Both were killed in their vehicles.

For many decades, US forces have had to protect themselves against terrorist attack while traveling in military and civilan vehicles. Many of these threats were concentrated in Europe and Latin America.

Terrorist tactics included ambushes using small arms fire and roadside explosives. Attacks using improvised explosive devices (IEDs) have dramatically increased in the last few years.

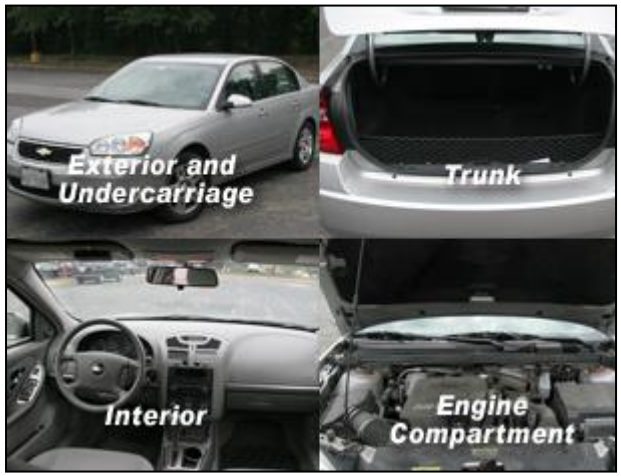
Ground Travel Fundamentals

A car burning after a terrorist attack in Greece.

Keep several measures in mind when considering vehicle security:

- **Do not draw attention to yourself.** Drive a vehicle that is common in the area. If possible, avoid using decals and bumper stickers that advertise your association with DOD.
- **Ensure your vehicle is well maintained.** A reliable vehicle is good for security and safety. Keep your tires properly inflated and the fuel tank at least half full.
- **Vary routes.** This makes it harder for terrorists to plan attacks. Do not be a predictable target.
- **Report suspicious behavior.** Be alert to unusual things, such as the absence of people in a market place. Alert your leadership and security officials immediately.

Inspecting Your Vehicle



The components of a vehicle you should examine during an inspection: the exterior and undercarriage, interior, the trunk, and the engine compartment.

Perform vehicle inspections for tampering or sabotage as local conditions warrant.

When you get a new vehicle, inspect it to familiarize yourself with its normal appearance so you can identify potential threats in the future. Then, inspect it whenever it has been in an unsecured location.

A good vehicle inspection consists of the following:

- **Visual exterior inspection:** Without touching the vehicle, look for any evidence of tampering on the undercarriage and in the wheel wells.
- **Visual interior inspection:** Without touching the vehicle, look though the windows for anything unusual on the seats or floorboards.
- **Complete interior inspection:** Look under the hood, in the trunk, in the glove compartment, behind the gas cap cover, under the seats, in the interior console – anywhere something may be hidden

You do not need to be an expert to perform a thorough inspection. Vigilance is the key.

Hotel Security Introduction

Ruins of the Paradise Hotel in Mombasa, Kenya following a 2002 VBIED attack.

Hotel security is a significant concern for the US government and host nation governments. In addition to low-level criminal activity, hotels have been targeted with small arms attacks, vehicle-borne improvised explosive devices (VBIED), and suicide backpack bombers.

Hotels are attractive targets for terrorists. They usually have lighter security than military installations or government buildings. They often attract guests who are potential targets such as affluent local nationals and Western officials and businessmen. Also, terrorists may perceive certain hotels as symbols of American influence or western economic power. Finally, many hotels employ third-country nationals for house staff and maintenance, further complicating security.

Selecting a Hotel

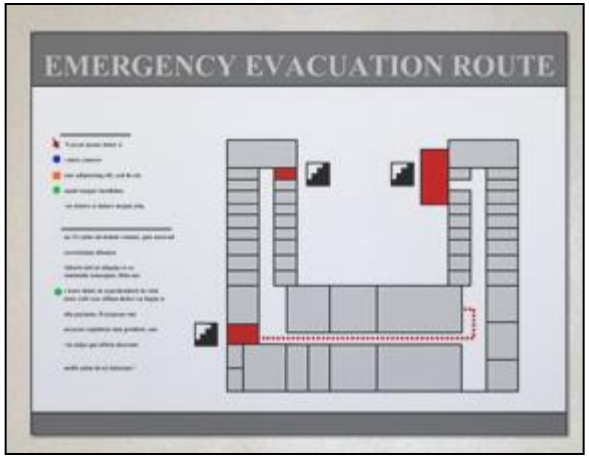
Smoke pours form the Taj Mahal Hotel in Mumbai, India after terrorists set fires to ensure as many casualties as possible.

When selecting a hotel, consider the following:

- Good stand-off from the street to protect from a VBIED
- Location in a non-violent and low-crime area
- Solid perimeter such as a steel fence, solid wall, and vehicle barriers
- Access control for both persons and vehicles
- Protection by hotel security personnel or host nation military
- Location near major roads for use in your daily commute
- Facilities inside the hotel such as a restaurant and gym to limit your need to leave during off-duty hours
- Electronic key card security to reduce vulnerability to crime

It may be hard to find a hotel that has all the security features you want. If so, look for security measures that protect against tactics previously used against hotels in the area.

Selecting Your Hotel Room



Floor maps marking the locations of emergency exits can usually be found on the back of a hotel room door.

Selecting a room can be important, though you may not have control of your room assignment. However, if you have the choice, consider the following:

- 3rd to 5th floor rooms are best – rooms on the 1st and 2nd floors are easily accessible from the outside, and rooms above the 5th floor are difficult to reach by emergency services
- A room away from the street can reduce your exposure to a VBIED
- Access to fire escapes and emergency evacuation routes

It may be hard to find a room with all of these characteristics. If you do not feel your room is safe, ask for another room or consider going to another hotel.

Inspecting Your Hotel Room

Night latches are commonly found in hotel rooms and should be used if available.

Once in your room, inspect it for security and make some mental preparations. Consider these things:

- Functioning locks on all doors and windows
- Risk of potential access through outside windows or a balcony
- Location of emergency exits and escape routes
- How to barricade yourself in your room – is the door solid, and can you move furniture around?
- Peephole to view visitors before opening the door
- A working phone

Be sure you can call the front desk and call directly to the US Embassy or US military HQ.

Also, when you leave your room, give it the appearance of being occupied:

- Leave the radio or television set on
- Hang the "Do Not Disturb" sign on the door
- Leave a light on in the area of the door

If you have concerns about your room's security features, consider asking for a different room or changing hotels.

Hostage Survival Introduction

Hostages may be taken for a variety of reasons and captivity may last for only a few hours or possibly for years.

The threat of kidnapping is a concern for DOD-affiliated personnel in many parts of the world. Hostages are taken to obtain political concessions, ransom, and publicity. Many hostage situations are resolved through negotiation or rescue. In some extreme cases, hostages are killed by their captors.

If taken hostage, your actions can improve your changes of survival. To prepare for this possibility, review "Isolated Personnel Guidance," an annex to CJCS Guide 5260. This is available from your Antiterrorism Officer.

Initial Response to Hostage Incident

In 1996, members of an insurgent group, MRTA, took hundreds of dignitaries hostage at the Japanese Ambassador's residence in Peru.

In the initial moments of a hostage taking, both the victim and captors are in a highly reactive mindset and prone to spontaneous actions. On one hand, an act to resist may be seen as a threat and met with deadly force. On the other hand, the chaos of the situation may afford an opportunity to escape. The decision to resist or comply is a personal choice you must make based upon your estimate of the situation and chances of survival.

However, if taken hostage, focus on defusing the situation:

- Control your fear and maintain your dignity; if you become excited, so will your captors
- Follow instructions of your captors
- Avoid sudden movements that your captors may view as hostile

The initial moments and hours of a hostage situation can be the most dangerous. Your decisions can increase your chance for survival.

Time In Captivity

The house where a US contractor, Thomas Hamill, was held captive in Iraq for 23 days before he escaped and was rescued by US Forces.

A hostage's time in captivity could last days, months, or years. During this time, you can expect sporadic to intense questioning about your DOD activities.

If questioned, consider the following:

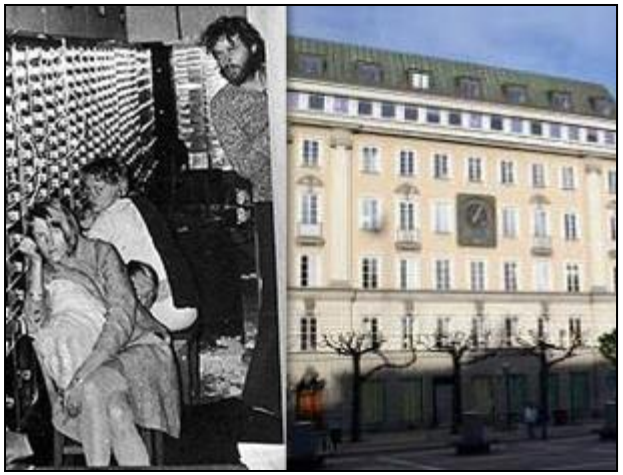
- Respond to your captors with respect and maintain your dignity
- Try not to display emotion or ego
- Avoid responding to questions about sensitive military matters
- Do not lie, but do not volunteer information; if a lie is necessary, keep it simple and be consistent.

Be prepared for a long captivity in poor conditions. It is important to maintain your mental and physical health:

- Keep active and maintain a daily routine
- Engage guards in conversation, but avoid topics such as politics and religion
- Eat the food that is provided to you even if it is poor quality
- Find ways to exercise
- Get enough sleep

Personal optimism, faith, self-discipline, and keeping the mind active are keys to enduring a difficult situation.

Stockholm Syndrome



The term "Stockholm Syndrome" comes from a 1973 bank robbery where hostages held for six days befriended their captor.

The "Stockholm Syndrome" is the behavior of hostages who, over time, become sympathetic to their captors.

Experts have identified factors in the development of Stockholm Syndrome:

- Credible threat to survival
- Perceived small kindness from the captor
- Isolation from perspectives other than the captor's

Hostages can become attached to their captor and begin to see the world from the captor's perspective. This can reduce their ability to see opportunities for escape or increase security.

If you become a hostage, remain true to your core values. You may develop rapport with your captor; however, you should never dismiss your needs, morals, and ideals. Remembering these principles will help you maintain objectivity in a dangerous situation and increase your chance of survival.

Hostage Resolution

Terry Anderson's release was finally negotiated after seven years of captivity in Lebanon.

If taken hostage, you have to decide if your best chance for survival is through remaining in captivity or attempting an escape.

If you do not feel there is an immediate threat to your life, your best option may be to remain in place and hope your release is negotiated or a rescue attempt made. In the event of a rescue attempt, be sure to:

- Immediately drop to the floor or dive behind a piece of furniture for cover
- After taking cover, do not make any sudden moves – you may be mistaken for a captor
- Do not attempt to assist rescue personnel – your actions may be misinterpreted as a threat
- Cooperate with rescue personnel – hostages may be handcuffed and detained while identifications are confirmed.

If you feel there is an immediate threat to your life, you may consider an escape attempt. Your chance for success is greatest when security is lighter, you know your location and which way to go for help, and you have food and water supplies for the environment.

CBRNE Introduction

First responders in protective gear during the 2001 anthrax attacks.

The chemical, biological, radiological, nuclear, and explosives (CBRNE) threat is a constant danger to DOD personnel and assets deployed throughout the world.

Terrorists have used Improvised Explosive Devices (IEDs) for decades, often with devastating results. Forms of IEDs include briefcase bombs, suicide bombers, and vehicle bombs.

While not common, chemical and biological attacks have also occurred. In 1995, terrorists attacked the Tokyo subway using Sarin nerve gas. In 2001, anthrax-laden letters were mailed to targeted individuals and places.

A nuclear or radiological attack has not yet occurred, but terrorist organizations are seeking new attack methods. The proliferation of nuclear materials that could be used as a weapon of terror greatly concerns US officials.

Responding to CBRNE Attacks

The anthrax laden letter mailed to Senator Tom Daschle during the 2001 anthrax attacks and first responders in protective gear in front of the Hart Senate Office Building.

The nature of a chemical, biological, radiological, or nuclear attack may be hard to determine. Chemical agents may be colorless, odorless, and difficult to identify. And, the effects of biological agents may take days or weeks to appear. Symptoms may resemble common ailments and may not be properly diagnosed.

Regardless of the type of incident, you can do several things to help protect yourself:

- Cover your body, especially your nose and mouth
- Wash any exposed part of your body with soap and water
- Seek medical attention as soon as possible
- Obey local authorities and first responders

If you believe a chemical attack is underway, move upwind into a well-ventilated area.

If you suspect a biological attack, avoid infected areas and watch for signs of illness in yourself and others.

In case of a radiological/nuclear attack, consider sheltering in place and tightly close doors and windows.

Responding to IEDs

A double-decker bus bombed during the July 2005 London IED attacks.

Be alert to the IED threat, even in areas without a history of attacks. Terrorists target symbolic sites, military personnel and equipment, innocent civilians, and first responders.

IEDs can be disguised as everyday items. Look for:

- Suspicious objects and packaging:
  - Unattended items that could conceal a bomb (suitcase, briefcase, flower planter, trash can, dead animal, parked cars)
  - Items with unusual batteries, wires, and strings
  - Recent construction or repairs (potholes, roadside mounds, building repairs)
  - Disturbed earth or depressions in the ground
- Suspicious behavior:
  - An unexplained decrease in local activity
  - Persons dressed in unseasonably warm clothing or behaving nervously

If you suspect an IED, clear everyone from the area and immediately alert local authorities or installation security.

Antiterrorism Individual Protective Measures

HOW *YOU* CAN FOIL TERRORISTS

OCJCS PC 5260, July 2012

A dynamic threat demands vigilance and discipline. This card offers techniques that limit opportunities to be targeted by terrorists. For detailed information, refer to CJCS Guide 5260, A Self-Help Guide to Antiterrorism.

GENERAL SECURITY ISSUES

Guard Information About Yourself and Job

- While off-base, limit signs of your DOD affiliation (wear civilian clothing, use non-descript vehicles).
- Limit access to personal information (name, rank, address, family).
- Practice OPSEC (need-to-know, secure comms., limited public conversations).

Be Prepared for the Unexpected

- Plan for the range of threats, avoid established or predictable patterns.

Recognize and Report Suspicious Activity

- Learn your surroundings and recognize behavior and items out of place.
- Remember descriptive details that may be useful to authorities.
- Report suspicious behavior and items to your chain of command, local authorities, or FBI.

INSIDER THREAT

Know Indicators of a Possible Insider Threat

- Anti-American statements asserting US policy and authority are illegitimate.
- Aggression or threats towards coworkers.
- Presence of unauthorized weapons.
- Attempts to communicate with US enemies.
- Association with extremist groups.
- Distribution of propaganda materials in support of an extremist position.
- Allegations of US persecution or prejudice against a minority group or religion.
- Repeated violation of policies.
- Abnormal mood swings or depression.
- Abuse of alcohol or drugs.
- Talk of suicide.

Report immediate violent threats to security or law enforcement immediately. If you believe a person may be mentally unstable, alert your supervisor or appropriate medical personnel.

TRANSIT SECURITY

Know Vehicle Security Measures

- Look for tampering around, under, and in your car.
- Keep doors locked and windows rolled up.
- Vary routes, travel times, and parking places.

Know Security Measures for Public Transportation

- Vary travel times, routes, and taxi companies.
- Match taxi drivers' faces to taxi licenses.
- Avoid crowded places on subway and train platforms and at bus stops.
- Secure doors on train sleeper cars.

Know Air Transit Security Measures

- Route through airports with good security.
- Clear security quickly at the airport.
- Remember that inside seats offer protection, but aisle seats offer options in an emergency.

TRAVEL SECURITY

Be Prepared for the Unexpected

- Ensure your Level 1 AT Training is current.
- Consult the DOD Foreign Clearance Guide.
- Receive an AOR specific Threat Briefing.
- Know location of the US Embassy and safe locations where you can find assistance.
- If possible, travel on a tourist passport.

Know Hotel Security Measures

- Consider hotels with good perimeter security, stand-off from the street, and access control points.
- Select an inside hotel room away from the street-side window, preferably on the 4th–10th floors.

OPSEC

Guard Information About Yourself

- Destroy all items that show your name, rank, or other personal information.
- Limit information posted on social networking sites concerning your family and job duties.
- Only discuss sensitive information with those that have a need-to-know, and only through the use of secure means.
- Be cautious giving out information regarding security measures and procedures.
- Report violations of OPSEC to your chain of command or appropriate authorities.

TELEPHONE SECURITY

If you receive a threatening phone call or Bomb Threat, dial *57 (verify local procedures), wait for the confirmation message that traces the caller, and then report the call to local authorities immediately.

RESIDENTIAL SECURITY

Know How to Protect Your Home and Family

- Consider removing your name and rank from your home and mailbox.
- Avoid the use of your name and rank on answering machines.
- Instruct family and associates not to provide strangers with information about you or your family.
- Brief family members on residential security and safety procedures.
- Ensure family members learn a duress word and keep it on file at your office.
- Advise associates or family members of your destination and planned time of arrival.
- Ensure residence has sufficient lighting, door and window locks, and barriers to meet the local threat.

Monitor family use of social networking sites to ensure OPSEC.

SUSPICIOUS PACKAGES

Be Prepared for the Unexpected

- Check mail and packages for:
  - Unusual odors (shoe polish or almond smell).
  - Protruding wires or strings.
  - Bulges, bumps, or odd shapes.
  - Oily stains on the package.
  - Too much wrapping
  - Excessive postage.
  - No return address or unfamiliar return address.
  - Differing return address and postmark.
  - Incorrect spelling or poor typing.
  - Appearance of foreign style handwriting.
  - Items sent "registered" or marked "personal".
  - Unusually light or heavy packages.
- Clear the area immediately and notify your chain of command and local authorities.