



---

# NAVAL SUPPORT ACTIVITY NAPLES ITALY

## SECURITY DEPARTMENT

---



## AT Level 1 Awareness Training



- Required annually for all assigned personnel to include military staff, DoD employees, contractors, and accompanying family members to locations outside of the United States. (OPNAVINST F3300.53C CNO Standard 25)
- Military/DoD Civilian: Complete via NKO or equivalent
- All others without CAC: Complete via JKO  
<https://jko.jten.mil/courses/at1/launch.html>



# Antiterrorism



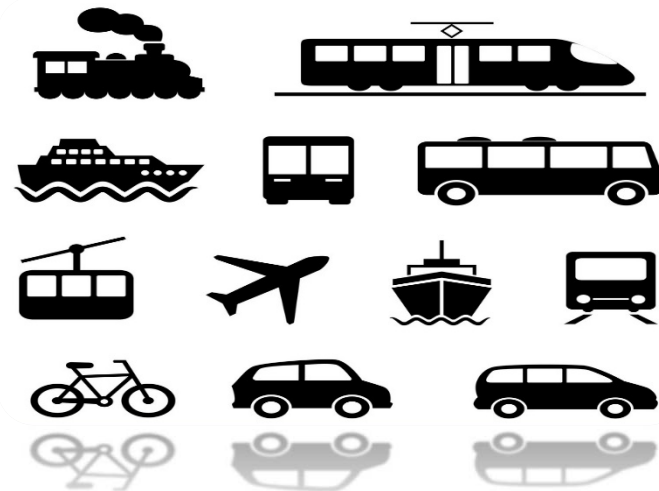
## GENERAL ANTITERRORISM INFORMATION

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, religious, or ideological.

### How Terrorists Select their Targets:

Consider ways you might become a victim of a terrorist attack. 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.
- Association:** Terrorists may focus on American tourists, personnel associated with the US Government, and individuals who appear to be high-ranking or important.
- Opportunity:** Terrorists look for "soft targets."





# Terrorist Planning Cycle Overview



**Terrorists prepare for and conduct attacks through predictable steps**

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

**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.

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

**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 attack method, obtain weapons and equipment, recruit specialized operatives, and design escape routes.

**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.

**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.

**Phase 7: Escape and 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.



# Be Vigilant



## Learn your environment and report suspicious behavior:

- Learn your environment so you recognize people and objects that are out of place.
- Be alert to strangers who are on government property for no apparent reason.
- Changes in local conditions, a decrease in activity by local citizens, and repetitious activities can be significant.
- Local citizens might hear rumors of violence and may change routines to maintain personal safety.

## Report Suspicious Behavior:

Report suspicious persons or activities near your home or office; provide a complete description of the person and/or vehicle to security officials.





# Be a Hard Target



**CDR USEUCOM Uniform policy:**  
Only authorized off the installation while commuting. Not allowed as a pedestrian or while riding a bicycle/moped/motorcycle.

## Do not be an easy target:

- Vary daily routines, such as departure times and routes to and from work.
- Remain low key and do not draw attention to yourself.
- Travel with a friend or in a small group.
- Refuse to meet with strangers outside your work place.

## Minimize exposure:

- Do not open doors to strangers.
- Select places with security measures appropriate for the local threat.
- Avoid places of high criminal activity.

## Clothing:

- Travel in conservative civilian clothing; do not wear distinct military items such as organizational shirts, caps, or military issue shoes or glasses.
- Do not wear US identified items such as cowboy hats or boots, baseball caps, American logo T-shirts, jackets, or sweatshirts.
- Wear a long-sleeved shirt if you have a visible US affiliated tattoo.



# Be a Hard Target



- **Travel:**
  - Avoid travelling in large groups
  - Avoid U.S. associated establishments
  - Sign up for STEP and DoS travel advisories.
  - Write down embassy/ consulate addresses and phone numbers.
- **Hotels:**
  - Place the “do not disturb” sign on the door and consider leaving the lights and television on when departing the room.
  - Keep room key cards hidden on your person.
  - Ask for rooms between the 3<sup>rd</sup> and 7<sup>th</sup> level, facing away from the street.
- **Vehicle:**
  - Select a plain car wherever possible.
  - If possible, vary routes to work and avoid isolated roads or late-night travel
  - Do not display or leave out military stickers or gear.
  - If you suspect you are being followed: Go to the nearest military base or police station.
- **Public Transportation:**
  - Only use taxis recommended by hotel staff.
  - Do not let someone you do not know direct you to a specific cab.
  - Ensure the taxi is licensed and the face of the driver matches the picture on license.



# Methods of Surveillance



- Surveillance may be conducted over a long period of time and employ various methods:
  - (1) **Stationary surveillance:** a common method in which operatives observe from a fixed location.
  - (2) **Moving surveillance:** conducted on foot or in vehicles.
  - (3) **Technical surveillance:** uses electronic means to record or gain access to security information.
  - (4) **Casual questioning:** used to elicit security information from approachable personnel.





# Suspicious Activity Report

- If you notice any suspicious activity, report it immediately. Do not rely on others to report the incident.

## Reporting Suspicious Activity

To report suspicious activity please contact your local law enforcement. Describe specifically what you observed, including:

- **Who** or **what** you saw;
- **When** you saw it;
- **Where** it occurred; and
- **Why** it's suspicious.

Report all suspicious activity to Emergency Dispatch:  
DSN: 626-5638  
Cell: +39-081-568-5638



# Active Shooter

How to respond to an Active Shooter in your vicinity:

## Option 1: Run/Escape

- Have an escape route/plan in mind.
- Spread the word.

## Option 2: Hide

- Hide in an area out of the active shooter's view.
- Block the entrance to your hiding place and lock the door.
- Silence all electronic devices.

## Option 3: Fight

- Only as a last resort.
- Act with physical aggression and throw objects at the active shooter.





# Insider Threat

- **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.
- **Pre-attack indicators of terrorism include:**
  - Anti-American statements asserting that US policy and authority is illegitimate.
  - Aggression or threats toward coworkers.
  - Presence of unauthorized weapons.
  - Attempts to communicate with US enemies.
  - Distribution of propaganda materials in support of an extremist position.
- **If you perceive an immediate/violent threat, alert security or law enforcement personnel immediately.**



# Improvised Explosive Devices (IED)



- **Improvised Explosive Devices:** IEDs can be disguised as everyday objects. Look for:
  - Suspicious objects and packaging
  - Unattended items that could conceal a bomb (suitcase, briefcase, flower planter, trash can, parked cars)
  - Items with unusual batteries, wires, cables, and strings
- **Be alert for suspicious packages:**
  - Unusual or unknown place of origin.
  - No return address.
  - Excessive postage.
  - Oily stains on the package.
  - Attached wires or strings.
  - Return address different than the postmark.
  - Peculiar odor. (Some explosives smell like shoe polish or almonds.)
  - Uneven balance or shape.
- **If you suspect a suspicious package, do not touch it.**
  - Evacuate the area and notify local authorities.



# Hostage Survival/ Personnel Recovery



- **General Considerations:**
  - Try to remain on the best terms with the captors possible, but be cognizant of the Stockholm Syndrome. Do not draw undue attention to yourself.
  - Prepare yourself for possible verbal and physical abuse, and lack of food, drink, and sanitary conditions.
  - Discretely observe your captors language, as well as clothing and unique physical characteristics.
- **Maintain Self-Control:**
  - The moment of attack is the point of maximum danger since your captors are most likely to panic or use excessive force.
  - Regain your composure and recognize your fear. Take mental notes of directions, times of transit, noises, and other factors to identify your location.
  - If you attempt an escape, plan your escape for times that maximize your chance of success. Recognize the moment when resistance is futile and stop when faced with deadly force.
- **While in Captivity:**
  - Exercise daily.
  - Read anything and everything.
  - Eat what is offered to you. You must maintain your strength.
  - Establish a slow, methodical routine for every task.
  - Stay mentally active.





# Hostage Survival/ Personnel Recovery



- **Dealing With Your Captors:**
  - Do not aggravate them.
  - Do not get into political or ideological discussions. Listen, but don't debate. Talk about: sports, family, clothing.
  - Comply with instructions, but always maintain your dignity.
  - Be proud of your heritage, government, and military association, but use discretion and don't be offensive.
- **Being Interrogated:**
  - If you must make up a story to protect sensitive information, make it a simple, believable story you will be able to remember and stick to it.
  - Give short answers. Talk freely about nonessential matters, but be guarded when conversations turn to matters of substance.
  - Be aware of “Good Guy/ Bad Guy” approach.
  - If forced to present terrorist demands to authorities, in writing or on tape, state clearly that the demands are from your captors.
- **During Rescue:**
  - Drop to the floor and be still. Avoid sudden moves. Wait for instruction.
  - Once released, avoid derogatory comments about your captors; such remarks will only make things harder for those still held captive.



# Defense Intelligence Agency (DIA) Terrorism Threat Levels



- DOD Terrorism Threat Levels. The Defense Intelligence Agency assesses a Terrorist Threat Level for each country. These Threat Levels inform DoD personnel of the need to take appropriate precautions.

**LOW:** No terrorist group is detected or the group activity is non-threatening.

**MODERATE:** Terrorists are present, but there are no indications of anti-US activity. The operating environment favors the host nation and the US.

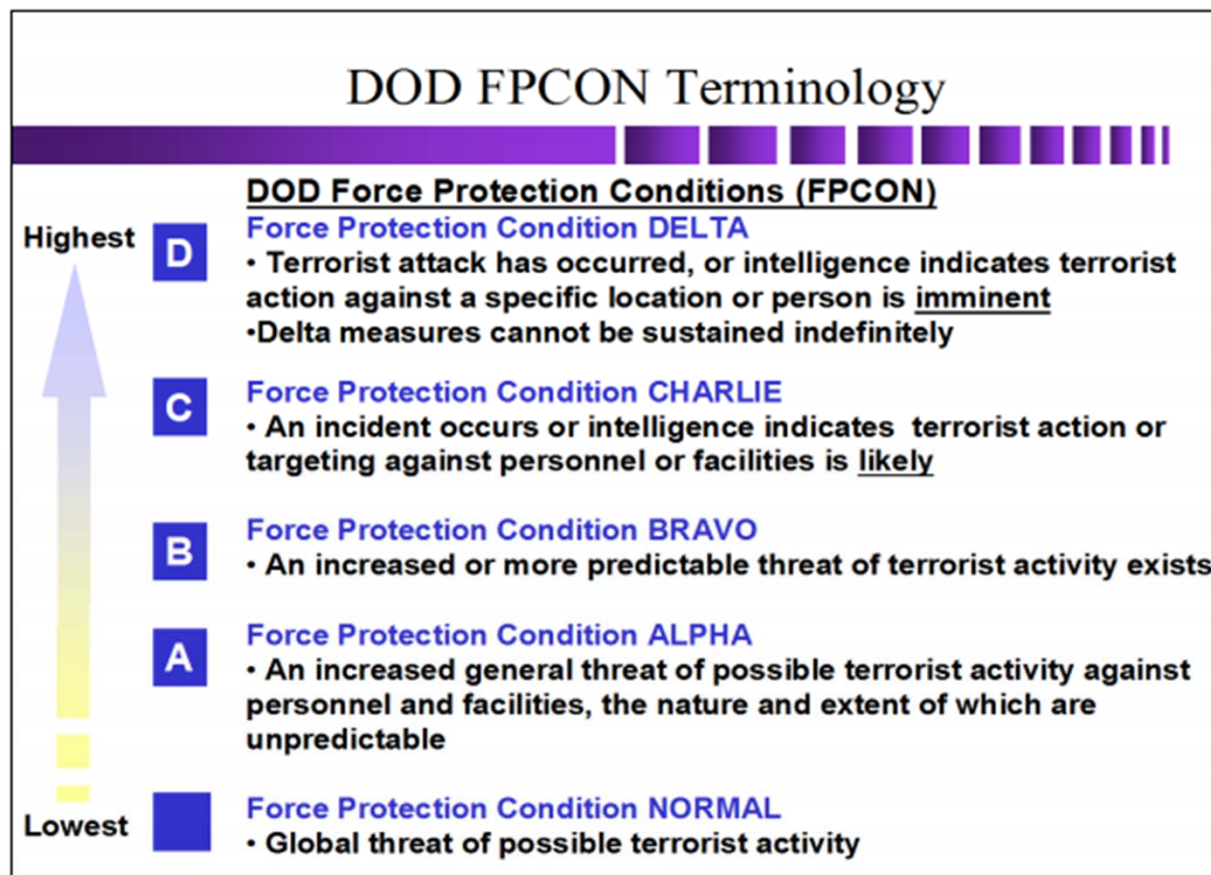
**SIGNIFICANT:** Anti-US terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty-producing attacks as its preferred method, but has limited operational activity. The operating environment is neutral.

**HIGH:** Anti-US terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. There is a substantial DOD presence and the operating environment favors the terrorist.



# Force Protection Conditions (FPCON)

- FPCONs are progressive levels of protective measures implemented by DoD installations or units in response to terrorist threats.





# Crime Prevention

- **Home Considerations**

- Restrict the possession of house keys. Lock all entrances at night, including the garage. Keep the house locked, even if you are at home.
- Destroy all envelopes or other items that show your name, rank, or other personal information. Remove names and rank from mailboxes.
- Keep yourself informed via media and internet regarding potential threats. (Department of State/ PAO)
- Develop an emergency plan and an emergency kit. Follow <https://www.ready.gov> kit guides.

- **Vehicle Considerations**

- Always lock your car
- Park in well-lit areas
- Don't leave valuables or other desirable items in the car. If items must be left in the car, remove from plain view.



# OPERATION IDENTIFICATION PROGRAM



- The Operation Identification Program is used in the assistance of identifying, recovering and returning stolen property to the rightful owner.
- Fill out the Operation ID Form:
  - Owner's Name
  - Description (Make/Model)
  - Serial Number
- Kept by Crime Prevention Manager to assist in the recovery of stolen property.
- Apply your own markings/numbers. Criminals often remove serial numbers.
- These forms are available from the Crime Prevention Manager. If you would like to complete these forms or have any questions please contact:

FC2 Dominguez: [Rebecca.Dominguez@eu.navy.mi](mailto:Rebecca.Dominguez@eu.navy.mi)

DSN: 626-5951/ COMM: 081-568-5951





# **IMPORTANT NUMBERS**

**NON-EMERGENCIES**

**081-568-5638/5639**

**EMERGENCY SERVICES**

**081-568-4911/5911**

**PROGRAM THESE NUMBERS IN  
ALL OF YOUR TELEPHONES**



# Useful Resources

- Department Of State (DoS) Travel Advisories: <https://www.travel.state.gov>
- AT Lvl 1 (non-CAC): <https://jko.jten.mil/courses/at11/launch.html>
- Foreign Clearance Guide (CAC only): <https://www.fcg.pentagon.mil/fcg.cfm>
- Smart Traveler Enrollment Program (STEP): <https://step.state.gov/STEP/>
- Antiterrorism Self Help Guide/ CJCS 5260 Manual:  
<https://www.jcs.mil/Library/CJCS-Guides/>
- Ready.gov: <https://www.ready.gov/>

**DON'T BE AFRAID!**

The information given during this briefing has been given with the intention of educating and enabling you to use these resources to be better prepared during your lives and travels.

Enjoy the many wonders Europe and the world have to offer!



# QUESTIONS?

**NSA Naples AT Distro email:**

**[M-NA-NSASECATFPMAILBOX-GD@OCONUS.NAVY.MIL](mailto:M-NA-NSASECATFPMAILBOX-GD@OCONUS.NAVY.MIL)**