Indicators of Terrorist Activity

Stopping the Next Attack In the Planning Stages

ANALYSIS of terrorist preparations for past attacks overseas and in the United States suggests that preoperational indicators may be present in the days or weeks prior to an attack. Indicators may point to possible terrorist planning. Alone, an indicator can result from legitimate commercial activity or criminal activity not related to terrorism; however, multiple indicators can suggest a terrorist threat.

Law enforcement officers should remain alert to potential indicators of pre-operational surveillance and planning activities. Information on suspicious or criminal activities potentially related to terrorism should be forwarded immediately to the local FBI Joint Terrorism Task Force – the FBI regional phone numbers can be found online at:

http://www.fbi.gov/contact/fo/fo.htm

and the Homeland Security Operations Center (HSOC), which can be reached via telephone at (202) 282-8101 or by email at: **hscenter@dhs.gov**

Indicators of Terrorist Activity

Table of Contents

Terrorist Surveillance and Planning

Excerpted from FBI Bulletin 144—August 27, 2004

The following indicators may suggest possible terrorist planning, particularly when they are observed at or near key facilities such as government, military, utility, or other high profile sites.

Alone, each indicator can result from legitimate recreational or commercial activities or criminal activity not related to terrorism; however, multiple indicators combined with other information can suggest a terrorist threat.

Surveillance and probing of potential targets is consistent with known practices of al-Qaeda and other terrorist organizations that seek to maximize the likelihood of operational success through careful planning.

Possible indicators of surveillance include:

- ►unusual or prolonged interest in security measures or personnel, entry points and access controls or perimeter barriers such as fences or walls
- ►unusual behavior such as staring or quickly looking away from personnel or vehicles entering or leaving designated facilities or parking areas
- ►observation of security reaction drills or procedures
- ►increase in anonymous telephone or email threats to facilities in conjunction with suspected surveillances incidents, indicating possible surveillance of threat reaction procedures
- ►foot surveillance involving two or three individuals working together
- ►mobile surveillance using bicycles, scooters, motorcycles, cars, trucks, sport utility vehicles, limousines, boats, or small aircraft.
- ►prolonged static surveillance using operatives disguised as panhandlers, shoe shiners, food or flower vendors, news agents or street sweepers not previously seen in the area
- ►discreet use of still cameras, video recorders or note taking at non-tourist locations
- ►use of multiple sets of clothing and identification or the use of sketching materials (paper, pencils, etc.)

The following indicators may suggest logistical planning for terrorist attacks:

- ►attempts to gain sensitive information regarding key facilities or personnel through personal contact or by telephone, mail, or email
- ►attempts to penetrate or test physical security and response procedures at key facilities
- ►attempts to improperly acquire explosives, weapons, ammunition, dangerous chemicals, flight manuals or other materials which could be used in a terrorist attack
- ►suspicious or improper attempts to acquire official vehicles, uniforms, badges, access cards or identification for key facilities
- ►presence of individuals who do not appear to belong in the workplace, business establishment or near a key facility
- ►behavior which appears to denote planning for terrorist activity, such as mapping out routes, playing out scenarios, monitoring key facilities, and timing traffic flow or signals
- ►stockpiling suspicious materials or abandoning potential containers for explosives (e.g.: vehicles or suitcases)

Suicide Bomb Attacks

Excerpted from FBI Bulletin 128—May 20, 2004

Suicide attacks can take numerous forms -- bombings (self-carried bombs or vehicle borne improvised explosive devices [VBIEDs]), shootings (attacker expects to die in the attack), and commandeering a vehicle

(displace operator and crash vehicle, causing casualties and potentially killing self in process).

Suicide bomb attacks may involve explosive-laden vehicles or individuals with a device carried on their person. The following are possible indicators that an individual is attempting to use his or her body as the delivery method for a bomb. Alone, each indicator can result from legitimate activities; however, multiple indicators can possibly denote a suicide bomber.

- wearing inappropriate attire such as loose or bulky clothing inconsistent with current weather conditions
- protruding bulges or exposed wires under clothing (possibly through sleeve)
- strange “chemical” odors
- sweating, mumbling (prayers), or unusually calm and detached behavior
- attempts to gain a position near crowds or VIP targets
- tightened hands (may hold detonation device)
- wearing disguises appropriate to target areas to elude detection. suicide bombers may disguise themselves with military, medic, firefighter, or police uniforms, or may pose as a pregnant woman

It is important to note that there is no clearly defined “profile” for a suicide bomber: men, women, and older children have all been suicide bombers.

Response Guidelines:

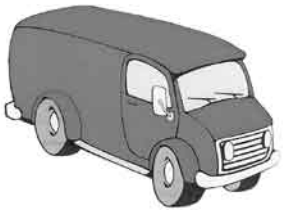
Law enforcement agencies should consider developing policies for responding to possible suicide bombing attacks. First responders should not attempt to negotiate with potential suicide bombers. Because the primary objective of suicide bombers is murder, they will likely attempt to detonate their device if they believe they have been discovered.

First responders should also search for secondary devices and associates of the suspect following the initial attempt or attack. A secondary device is an explosive item or device designed to function after the first device has exploded. They may be hidden in everyday objects such as vehicles, briefcases, flower pots, garbage cans, etc., and are usually detonated less than one hour after the initial attack, targeting first responders as well as the general population.

A second suicide bomber may also attempt to detonate a follow-up blast to kill responders and bystanders.

First responders should scan any bystanders for individuals who may be supporting the suspect.

Countermeasures include operational planning--devising possible attack scenarios (defining relevant threats and establishing concentric rings of security); breaking routines (decoy motorcades, irregular security checks and patrols); screening individuals; and controlling crowds.



Vehicle-Borne IEDs

Excerpted from FBI Bulletin 125—April 30, 2004

Terrorist operatives worldwide will likely continue to rely on vehicle-borne improvised explosive devices (VBIEDS) as a method of attack. The following indicators may point to possible terrorist planning. Alone, each indicator can result from legitimate commercial activity or criminal activity not related to terrorism; however, multiple indicators combined with other information can possibly suggest a terrorist threat or an impending VBIED attack.

Suspicious attempts to modify equipment may provide a possible indication of pre-operational activity. Transactions and modifications may include:

- theft or purchase, particularly cash purchases from private individuals, or large delivery vehicles, vans, cargo containers, trailers, or related equipment
- purchasing inquiries related to commercial delivery or utility vehicles by individuals who seem to lack industry knowledge, credentials, or experience
- vehicles that have been modified to handle heavier loads, create additional storage areas, or increase fuel capacity or vehicle speed
- discovery of batteries, wiring, timers or other power supply or switching components in the passenger compartment of a vehicle
- theft or purchase of paint or decals, or the discovery of painting patterns similar to those found on delivery, security, emergency, response, or utility vehicles

- theft or purchase of specialized fuels, agricultural or industrial chemicals, blasting caps, or fuses for explosives
- theft or purchase of respirators or chemical mixing devices
- attempts to purchase or steal facility blueprints

Certain characteristics of training could represent a potential terrorist interest in VBIED attacks. These training indicators include:

- Commercial Driver's License students who do not seem interested in finding employment
- reports of semi-truck or large vehicle driving training conducted by uncertified individuals, particularly in remote areas or at night
- rescues made from burning buildings or vehicles where the victims seem reluctant to provide details or give inconsistent versions of events
- attempts to avoid reporting or to restrict access of first responders to fires or minor explosions in residences or storage facilities
- reports of explosions or unexplained fires in remote, rural or vacant industrial areas
- patients displaying burns or chemical exposure symptoms who provide vague or irrational explanations as to the circumstances surrounding the injuries

Surveillance and probing of potential targets is consistent with known practices of Al-Qaeda and other terrorist organizations that seek to maximize the likelihood of operational success through careful planning. Possible indicators of surveillance include:

- physical surveillance, which may include videotaping or attempts to photograph potential targets, particularly focusing on access points
- loitering near restricted areas or sensitive sites
- reports of persons approaching security checkpoints with unusual requests, such as asking for obscure directions, or otherwise attempting to distract security personnel
- reports of individuals attempting to make unscheduled deliveries or "complimentary" maintenance visits – particularly if the vehicle appears too large to meet facility clearance levels
- "dry runs" of routes to identify speed traps, road hazards, or bridges and overpasses with clearance levels too low to accommodate large vehicles
- incidents involving ramming or bumping of physical security barriers or the unauthorized parking of vehicles on or near facility property

Logistical planning for VBIED attacks may include characteristics such as:

- rental, delivery or utility vehicles parked in unusual locations such as fields, vacant warehouses, or other secluded areas
- suspicious behavior by residential occupants or storage unit customers when approached by rental employees, security personnel or neighbors
- unusual deliveries or frequent off-hours visits to storage units or remote storage sites
- complaints of unusual fumes, liquids, residue or odors from neighboring storage unit customers
- suspicious employment attempts at sensitive sites, vehicle dealerships, rental agencies, delivery companies, security agencies, and emergency services or freight hauling companies

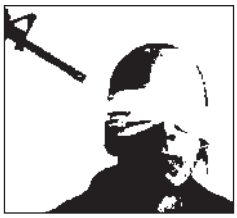
Operational indicators of a VBIED attack may include characteristics such as:

- drivers who operate the vehicle in an overly cautious manner, attempt to abandon the vehicle or seem overly cautious about accessing the cargo area
- delivery or utility vehicle drivers who seem nervous or display non-compliant behavior such as insisting on parking close to a building or restricted area
- delivery vehicles that lack a sufficient number of people to conduct the stated purpose of the visit; for example, a solo driver with a semi-trailer sized delivery
- excessive vehicle weight or unusually uneven weight distribution; for example, the vehicle leans to one side or appears overloaded
- smoke, strong chemical, or fuel odors emanating from a vehicle

A VBIED attack may be pre-empted if law enforcement and security personnel at key facilities such as govern-

ment, military, utility or other high profile sites re-examine existing counterterrorism procedures and incorporate protective measures to include:

- review existing vehicle bombing prevention procedures to incorporate thwarting the use of a moving vehicle bomb, and consider adjusting buffer zones further from potential targets
- periodically rearrange exterior vehicle barriers traffic cones, and road blocks to alter traffic patterns near facilities
- limit the number of access points and strictly enforce access control procedures
- approach all illegally parked vehicles in and around facilities, question drivers and direct them to move immediately; if the owner can not be identified, have the vehicle towed by law enforcement
- provide vehicle inspection training to security personnel, and institute a robust vehicle inspection program to include checking the undercarriage of vehicles, under the hood and in the trunk
- deploy explosive detection devices and explosive detection canine teams
- institute/increase security patrols varying in size, timing and routes
- increase perimeter lighting and maintain/remove vegetation in and around perimeters
- encourage personnel to be alert and to immediately report any situation that appears to constitute a threat or suspicious activity
- guard force turnover and personnel authentication procedures
- implement random security guard shift changes
- deploy visible security cameras and motion sensors
- review security camera footage daily to detect possible indicators of pre-operational surveillance.



Kidnapping

Excerpted from online sources

Recent headlines have highlighted the kidnapping of Americans and allies by terrorists overseas, often with dire consequences.

Kidnapping usually takes place in public areas; in a hotel or residence; or from your car. In virtually all cases a weapon will be used to force your cooperation and a car will be used to take you away to the final destination of your captors.

One common method of kidnapping is to stop a victim's car as it is driving along a predictable route. That's why it is important to vary your route frequently.

You might be kidnapped while driving to or from work. Usually you will be under surveillance for several days before the kidnapping.

Stay alert for the following indicators that someone nearby is stalking you:

- Illegally parked vehicles
- Occupied parked vehicles
- Vehicles that move with you
- Vehicles that pass, then park
- Erratic moves/driving
- Vehicles slowly maneuvering through turns and intersections
- Vehicles signaling for turns but which do not turn
- Running through red lights
- Flashing lights between cars
- Pausing in traffic circles until target exits
- Speeding up/slowing down
- Same vehicle day after day, particularly if occupied
- Different vehicles occupied by the same people

Check occasionally to see if another car is following you. If you think you are being followed, circle the block or change directions several times to confirm the presence of surveillance.

Write down a description of the car and its occupants, if possible. It is okay to let the surveillants know you have

seen them, but do not under any circumstances take any action that might provoke them or that could lead to confrontation. If they do not stop following you, drive directly to the nearest safe haven. Carry a cell phone. Learn to recognize and be alert to events that could signal the start of a plan to stop your car and take you captive:

- a cyclist falling in front of your car
- a flagman or workman stopping your car
- an unusual detour
- a fake police or government checkpoint
- road blocked by a disabled vehicle or accident victim
- an accident in which your car is deliberately struck
- cars or pedestrian traffic that box you in

Rental Vehicles

Excerpted from FBI Bulletin 139—August 6, 2004

The following indicators may point to possible planning to use rental vehicles in a terrorist attack.

- customers who attempt to give vague or unverifiable references or employment information on rental agreements, who insist on paying in cash and/or who seem overly concerned about privacy

- attempts to expedite collection of deposits made on rental vehicles reported as "stolen"

- suspicious inquiries concerning weather vehicles can be modified to handle heavier loads, create additional storage areas or increase fuel capacity or vehicle speed

- suspicious inquiries concerning the use of limousines by private drivers or limousine's exact length, height or interior volume

- reports of rental vehicles parked for prolonged periods of time near sensitive facilities such as government, military, utility or other high profile sites

- suspicious attempts to gain employment at vehicle dealerships and/or rental agencies

- customers displaying burns or chemical exposure symptoms who provide vague or illogical explanations as to the circumstances surrounding the injuries

- returned rental vehicles with altered company logos, department of transportation numbers, or structural or appearance modifications

When reporting suspicious incidents, car, truck and limousine rental company employees should provide as much detailed information as possible on:

who:

- name
- date of birth
- driver's license number
- passport number
- description
- citizenship

where:

- name of rental facility
- place where vehicle was sighted or parked
- list various locations if activity was moving

when:

- date and time of activity

what:

- describe the activity, particularly what made it suspicious

Terrorism Financing

Excerpted from FBI Bulletin 132—June 17, 2004

Investigation into terrorist financing is an important component of overall U.S. counterterrorism investigative efforts. The FBI has compiled the following list of potential terrorism financing indicators and other reportable items to assist agencies in recognizing activities of terrorists and their support networks.

Although patterns of conduct consistent with the indicators may point to criminal activity, they may not necessarily be linked to terrorism. Indicators of money laundering, for example, are often similar to indicators of terrorists' financial transactions.

Characteristics of Terrorist Suspects:

- engage in activities in the U.S. that do not match the stated purpose of their visas

- sponsor visas for persons with known or suspected ties to terrorism
- arrange marriages to facilitate U.S. citizenship
- have difficulty providing personal background information beyond that contained in documents carried on-person or a seemingly practiced set of facts
- can provide no record of travel to the country to which the individuals hold a valid passport
- exhibit unusual concern for secrecy, particularly with respect to their identity, type of business, or property held
- possess vague knowledge of the amount and details of a transaction or offer inconsistent or confusing details about the transaction
- unwilling to provide explanation of financial activity
- over-justify or explain transactions; are nervous, secretive, reluctant to meet in person; provide confusing details of transactions or show uncommon curiosity about internal systems, controls and policies
- lifestyle not consistent with known, legitimate sources of income
- change addresses frequently–use multiple post office boxes
- possess large sums of money not consistent with known income sources
- buying or renting goods, services, vehicles, accommodations with cash or by fraudulent means, or otherwise using false identification or indirect ownership
- engage in sudden withdrawal of funds or closing of accounts with accompanying wire transfers to foreign accounts

Characteristics of Methods Used to Finance Terrorist Operations

1. Exploitable banking patterns and account profiles

- accounts opened with cash or equivalent in the average amount of $3,000 to $5,000; individual refuses to provide information required by the financial institution or attempts to reduce information provided to a level that is misleading or difficult to verify
- multiple suspicious financial transactions initiating from or terminating at the same location
- large wire transfers to or from U.S. financial accounts to accounts in the Middle East or other volatile areas
- bank accounts show indicators of “structuring”
- unexplainable clearing or negotiation of third-party checks and their deposits in foreign bank accounts
- corporate layering: transfers between bank accounts of related entities or charities for no apparent reason
- wire transfers by charitable organizations to companies located in countries known to be bank or tax havens
- transactions with no logical economic purpose (no link between the activity of the organization and other parties involved in the transaction)
- large currency withdrawals from a business account not normally associated with cash transactions
- use of multiple individuals to structure transactions under the reporting threshold to circumvent reporting requirements and then to funnel funds to a foreign beneficiary
- use of a business account that would not normally generate the volume of wire transfer activity into and out of the account
- same-day transactions at the same depository institutions at different teller windows
- apparent intent to circumvent wire remittance company’s internal requirements for presentation of identification through purchase of money orders in small amounts
- import/export business acting as an unlicensed remitter to conduct wire transfers
- individuals/businesses serving as intermediaries in the wire transfer process
- beneficiaries of wire transfers involving a large group of nationals of countries associated with terrorism
- known terrorism-associated charity or relief organization linked to the transactions
- wire transfer activity within a short period following deposits
- beneficiary account in problematic country
- currency exchange: buying and selling foreign currencies from countries in the Middle East or Persian Gulf

- transactions at a level not commensurate with stated occupations
- lack of apparent fund-raising (small checks or typical donations) associated with charitable bank deposits
- use of sequentially numbered money orders
- opening accounts in groups of three or four individuals, or opening accounts joined with other accounts
- opening an account for which several persons with no apparent familial or business relationship have signature authority
- sudden deposit(s) into dormant account containing a minimal sum, followed by daily cash withdrawals that continue until the transferred sum is removed
- use of multiple individuals to structure transactions under the reporting threshold
- repetitive round-denominations deposits or withdrawals
- checks made out to cash
- memo lines on checks identify other accounts or assets

2. Funding distribution

- general avoidance of traditional banking systems
- use of messengers to transmit funds
- unauthorized redirection of funds by staff members of apparently legitimate organizations to financial accounts, individuals or organizations with known or suspected terrorist links
- changes in patterns of transactions, including trading on financial and commodities markets
- large wire transfers to or from U.S. financial accounts to accounts of known or suspected terrorists
- individual is associated with person linked to document forgery

3. Communication methods

- establishment or maintenance of Web sites which support terrorist activities and contain anti-U.S. rhetoric
- use of Internet cafes known to be frequented by extremists
- e-mailed instructions to operatives not to use a method of communication that has been detected by law enforcement or the intelligence community
- use of web sites which solicit recruits for Jihadist activities; or that warn specific ethnic groups to leave or avoid visiting certain areas
- use of messengers to transmit messages and electronic media
- use of pre-paid, disposable cellular phones

AgroTerrorism

Excerpted from FBI Bulletin 87—October 8, 2003

Al-Qaeda and other international terrorist groups continue to express an interest in agroterrorism as a means of attack. An agroterrorism attack is the intentional release of pathogens to destroy or damage livestock or crops. Such an attack could inflict significant economic damage; instill fear in consumers; and lower confidence in U.S. safety.

Differentiating between a natural or man-made disease outbreak remains a major challenge to defend against an agroterrorism attack. The use of agroterrorism tactics under the cover of a naturally occurring epidemic provides an attacker with deniability, as an agroterrorism attack can be virtually indistinguishable from natural outbreaks and can be difficult to connect to a terrorist group.

While not exhaustive, the following list suggests possible indicators of agroterrorism:

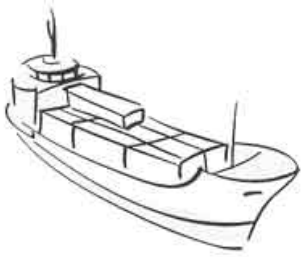
- the purchase, loss, or theft of cultures, toxins, vaccines, and medications
- inquiries about obtaining agricultural pathogen samples
- unusual purchases or unexplained thefts of animals or

agricultural equipment, such as commercial sprayers

- shipments of supplies from laboratory companies that include growth media (i.e., culture dishes)
- the storage of biological and agricultural equipment in apartments, houses, or garages. these items may include laboratory materials, protective clothing (i.e., surgical masks, gas masks, rubber gloves, self-contained breathing apparatuses), incinerators, incubators, cell cultures, agricultural sprayers, improvised showers and eye baths in unusual locations, and textbooks and journals discussing biology, chemistry, explosives, and poisons
- noxious or unusual odors, similar to a brewery or fermented grain, not routinely associated with the area
- unusual travel to areas where agricultural or livestock disease outbreaks have occurred or where there is a current epidemic
- suspicious spraying during periods of darkness
- an unexplained increase in the number of sick or dying animals
- suspicious activities at or near livestock feedlots, processing plants, or poultry plants

Examples of other suspicious behaviors that may indicate a possible agroterrorism plot include:

- purchasing large amounts of highly toxic pesticides with cash
- asking specific questions about the toxicity of a pesticide
- making suspicious inquiries regarding equipment (i.e., tank size, spray range, etc.)
- loitering near pesticide storage areas
- presenting unusual (possibly altered) documents, including fraudulent pilot's or truck driver's licenses, false shipping or purchasing papers, and other forms of false identification



Maritime Activity

Excerpted from FBI Bulletin 116—March 10, 2004

In recent years, a number of incidents have occurred involving suspicious individuals possibly conducting surveillance of port facilities, cruise ship docks, naval bases, dams, bridges and power facilities in the U.S.

Maritime attacks represent an attractive option for terrorists. Operations could be organized and launched by a small number of individuals using commercially available equipment. Reporting indicates incidents in which suspicious individuals have queried marine shops and schools concerning equipment and training. The following indicators may point to possible terrorist planning:

- requests for specific specialty training, including odd inquiries that are inconsistent with recreational diving requests to learn the advanced skills associated with combat swimming, including training with rebreathers, deep diving, conducting "kick counts" or receiving navigation training
- rapid progression of professional association of diving instructors (padi) training and certifications, particularly if the training is routinely conducted between the same two or three individuals
- training sponsored by groups or agencies not normally associated with diving
- training given by instructors who do not advertise and appear to have little means of visible support, especially those with a history of extremist views
- training conducted in remote or atypical locations or restricted areas
- threats, coercion, or attempts to bribe trainers for certification

Suspicious attempts to purchase specialized maritime equipment may provide a possible indication of preoperational activity. Transactions may include:

- individual purchases of common dive gear without the required certifications, or attempts to rent gear inconsistent with the stated purpose of the diving trip.

- volume purchasing inquiries related to swimmer delivery vehicles (SDVs) and diver propulsion vehicles (DPVs).

- exclusive purchases of darkened gear, or after-market painting attempts to purchase large magnets, large diameter PVC pipe, or empty compressed gas cylinders (or theft of same) and attempts to purchase advanced gear, such as rebreathers or other equipment used in mixed gas diving, by individuals who appear to lack expertise in the use of the equipment.

Logistical planning for scuba attacks may include characteristics such as:

- groups of individuals, especially those with no visible means of support, sharing a common address near the water

- attempts to take diving equipment, particularly advanced gear, without the required certifications, on commercial flights

- cash purchases of small boats or personal watercraft from private individuals

- invalid or unusual explanations of visitor, employment or student status and employment attempts at diving equipment dealers or rental shops

Surveillance and probing of potential targets is consistent with known practices of Al-Qaeda and other terrorist organizations that seek to maximize the likelihood of operational success through careful planning. Possible indicators of surveillance include attempts to photograph or loiter near restricted areas or sensitive sites and attempts to gain employment at sensitive sites or with outside vendors offering access to these sites.

The Department of Homeland Security recommends that agencies having jurisdiction over harbors, ports and waterways consider taking precautionary measures, such as use of surface and underwater lighting and increased patrols, to further enhance maritime security. Law enforcement agencies should forward threat information related to maritime or coastal interests or information on suspicious surveillance, inquiries or scuba-related purchases to the nearest FBI Joint Terrorism Task Force.

Floating Devices and Improvised Mines

Excerpted from FBI Bulletin133—June 24, 2004

Traditional seaborne mines have been used to offset military superiority, interdict enemy maritime logistics, disrupt an adversary's maritime commerce, or deny use of a waterway, coastal area or facility.

Although large scale, military style mining operations against the U.S. are assessed to be beyond the capabilities of transnational terrorists, the technological sophistication demonstrated in evolving improvised explosive device (IED) construction raises the possibility of limited, geographically dispersed waterborne IED attacks.

Analysis of recent incidents involving floating IEDs have revealed no significant similarities in construction, suggesting these are isolated cases involving individuals rather than incidents of transnational terrorism.

Nonetheless, these incidents demonstrate potential vulnerabilities, and the possibility exists that extremists may choose similar tactics to conduct attacks against the U.S. maritime infrastructure.

Designs used in floating IEDs have included:

- combinations of IEDs and styrofoam blocks

- inner tubes or rafts carrying IEDs onboard

- sealed PVC pipes with IEDs attached or encapsulated inside

- IEDs attached to floats or buoys

- vehicle-borne IEDs using drifting or unmanned boats

- IEDs concealed in floating debris such as plastic or rubber containers and trash bags

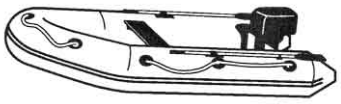
Potential indicators related to planned floating IED or terrorist mine attacks:

- reports of suspicious requests for hydrographic charts associated with naval or commercial port facilities

- evidence suggesting trends or patterns in terrorist

related hoaxes or threat reporting dealing with mines, floating IEDs, etc.

- reports of suspicious inquiries concerning mine countermeasures, "Q routes" (a system of preplanned shipping lanes in mined or potentially mined waters used to minimize the area that mine countermeasures forces have to keep clear of mines to provide safe passage for friendly shipping), and other defensive security measures for naval or commercial port facilities.
- evidence of IED designs that may lend themselves to conducting waterborne attacks
- reports of attempts to purchase or steal large magnets, large diameter PVC pipe, empty compressed gas cylinders, large styrofoam blocks, or watertight storage drums
- evidence of attempts to camouflage possible floating IED components by painting,, encasing in innocuous appearing items or materials, etc.
- reports of launching or retrieval of boats from unusually remote areas
- reports of boating activities conducted in atypical locations or attempts to loiter near restricted areas
- reports from vessels or coastal residents of small explosions
- evidence of vessel damage indicating heavy objects may have been rolled over the side or the presence of unusual ramps or rails on the decks of vessels
- evidence of attempts to conduct underwater topography of sensitive areas, commercial port facilities, or waterways
- annotated nautical charts or other evidence possibly indicating plans to deploy possible mines near geographic chokepoints, commercial shipping lanes, or port facilities
- reports of abandoned small boats found adrift near sensitive sites
- reports or incidents involving unusual or unidentified floating objects near vessels or in harbors, ports, or commercial waterways
- reports of unexplained explosions or unusual fouling incidents (such as unidentified objects attached to cables or ropes wrapped around screws, etc.) involving vessels operating near harbors, ports, or commercial waterways
- reports involving vessels conducting nighttime dumping of heavy objects near harbors, ports, or commercial waterways
- reports involving aircraft dropping objects over water (particularly at night) near harbors, ports, or commercial waterways



Small-Boat Attacks

Excerpted from FBI Bulletin 86—October 1, 2003

Explosive-laden boats represent a threat to U.S. maritime interests. Terrorists can convert an innocuous small craft into an effective weapon.

Deceptive tactics, such as disguising the small boat as a local security vessel, will continue to be the terrorist mainstay; however, tactics involving more than one boat may also be used to overcome a targeted vessel's defenses. The following indicators may point to possible terrorist planning.

Certain characteristics of training could represent a potential terrorist interest in small boat attacks. These indicators include:

- reports of high-speed, close-aboard runs of one or more small boats towards large draft merchants or other vessels restricted in their ability to maneuver, particularly in remote locations near geographic choke points
- reports of small boats following closely in the wake of a large draft vessel, especially during hours of darkness
- dangerous maneuvering and other suspicious incidents recently associated with the same two or three individuals
- launching or retrieval of boats from unusually remote areas
- boating activities conducted in atypical locations or attempts to loiter near restricted areas
- reports of gunfire or small explosions by local vessels or coastal residents and rescues made from a sunken or stranded vessel where the victims seem reluctant

to describe details or who give inconsistent or conflicting versions of what happened

Suspicious attempts to purchase or modify equipment may provide a possible indication of pre-operational planning activity. Transactions and modifications may include:

- individual purchases, particularly cash purchases, of several small boats, personal watercraft, outboard engines, gasoline tanks, or related equipment from private individuals or small businesses
- purchasing inquiries related to small commercial or fishing vessels by individuals who seem to lack industry knowledge, credentials, or trade experience
- attempts to purchase numerous fishing and waterfowl hunting licenses or recreational marine permits by a single individual, particularly if the purchaser is not related to the licensees or is not associated with maritime tourism, marine dealerships, outdoor guiding services, or charter boat fishing businesses
- individual purchases of paint or decals similar to those found on local security or port services vessels by those without authority to do so, or the theft of same
- discovery of painting patterns fashioned to resemble those of local security or port services vessels
- theft or purchasing attempts of harbor security or port services uniforms, access badges, or related equipment
- maintenance requests that involve unusual structural modifications (e.g. removal of seating, important fishing-related equipment, etc.), especially those that seem to reduce the ability of the vessel to perform in its normally expected role and demands to create additional voids or storage areas below decks, to dramatically increase fuel capacity or vessel speed, or to place vertical metal plates (or other possible shrapnel producing materials) below decks or near the bow

Logistical planning for small boat attacks may include characteristics such as:

- groups of individuals, especially those with no visible means of support, sharing a common address near the water and invalid or unusual explanations of visitor, employment or student status.
- surveillance and probing of potential targets is consistent with known practices of al-qaeda and other terrorist organizations that seek to maximize the likelihood of operational success through careful planning.
- possible indicators of surveillance include attempts to photograph or loiter near restricted areas or sensitive sites and attempts to gain employment at sensitive sites, security detachments, or with outside vendors offering access to these sites.

Helicopter Attack

Excerpted from FBI Bulletin 141—August 6, 2004

Al-Qaeda has apparently considered the use of helicopters as an alternative to recruiting operatives for fix-wing aircraft operations. Terrorists may view helicopters as an attractive weapon due to their maneuverability and non-threatening appearance when flying at low altitudes in urban environments. Recent reporting indicates that Al-Qaeda may be targeting key financial institutions in New York City, New York, Northern New Jersey, and Washington, D.C., with the intention of dealing a severe blow to the U.S. economy.

Possible attack scenarios in the United States could involve Al-Qaeda operatives seeking out vulnerabilities in security procedures to hijack commercial helicopter flights.

Operatives may also contract a flight from a charter or tour service to facilitate a hijacking. Helicopters could be used in suicide attacks against high-profile ground targets or to attack the public in open areas, including parades and sporting events, with explosives carried on board to increase the destructive effects.

Helicopters could conceivably be used to introduce chemical or biological weapons into high-rise building ventilation systems, which may be more easily breached from the roof than from lower floors. Aerial spraying equipment used to disperse fertilizer or insecticide could be used to efficiently deliver these toxic substances.

During authorized searchers, law enforcement officers should take note of helicopter-related images, including photographs of interiors and exteriors of rotary-wing aircraft, helicopter tour company brochures, and accompanying aerial photographs of economic and commercial centers

Law enforcement agencies should also maintain liaison with commercial and private helicopter operators and encourage them to report suspicious incidents and inquiries. Helicopter flight school operators should also be alert to and report suspicious inquiries, such as undue interest in helicopter operations, payloads, and security procedures.

Private sector owners and operators as well as pilots and maintenance crews should undertake the following protective measures:

- enforce thorough screening of passengers and require identification of all passengers, especially escorted groups, prior to boarding charter flights and tours
- verify that baggage and cargo are known to the persons on board
- establish and enforce employee identification measures fro aircraft maintenance, refueling, service, and delivery personnel and others who may have contact with aircraft or passengers
- report loitering in vicinities of aircraft or air operations
- report suspicious inquiries into aircraft and aircraft operations, and suspicious incidents involving individuals taking photographs, videos, or notes of aircraft
- report personnel impersonating pilots, security personnel, emergency medical technicians, or other personnel using uniforms or vehicles as methods to gain access to aviation facilities or aircraft.
- enforce current physical security standards at airports, heliports, and helipads. fix broken or defective doors, gates, and locks that secure access to parked helicopters, and refueling and maintenance areas
- establish physical barriers in passenger boarding areas to restrict unauthorized persons from accessing helicopters or areas of aircraft operations
- install magnetometers in passenger boarding areas to discourage passengers from carrying weapons or dangerous items on board charter or tour helicopters.

Self-Storage Facilities

Excerpted from FBI Bulletin 140—August 6, 2004

Intelligence indicates Al-Qaeda may be planning an attack using improvised explosive devices (IEDs). Historically, terrorist plots involving IEDs have utilized self-storage facilities to house bomb components and supplies or assemble devices prior to an attack.

The following indicators may point to possible terrorist use of self storage units to facilitate an attack. Suspicious activity by self-storage customers may provide a possible indication of pre-operational activity. Behaviors of concern include customers who:

- insist on paying in cash, sometimes weeks or months in advance
- seem overly concerned about privacy
- visit the storage facility late at night or at unusual times
- exhibit suspicious behavior when approached by rental company employees and security personnel
- have unusual fumes, liquids, residues or odors emanating from the storage units
- display burns or chemical exposure symptoms and provide vague or irrational explanations for the injuries
- discard chemical containers in storage unit dumpsters

Storage of the following items may indicate logistical planning for a terrorist attack:

- Quantities of fuel
- Agricultural or industrial chemicals
- Agricultural equipment, such as commercial sprayers
- Explosives, blasting caps, or fuses
- Weapons or ammunition
- Flight manuals or similar materials

- Laboratory materials (e.g., flasks, sealed containers) or protective clothing (e.g., surgical masks, gas masks, rubber gloves, self-contained breathing apparatuses), incinerators, incubators, cell cultures, agricultural sprayers, improvised showers and eye baths, and textbooks and journals discussing biology, chemistry, explosives and poisons

- Pesticides

- Large delivery vehicles, vans, cargo containers, trailers or related equipment

Law enforcement officers are encouraged to maintain liaison with owners and employees of storage facilities in their respective jurisdictions and ask them to report suspicious activities. In any case where suspected bomb components, chemicals or radioactive materials are encountered in an investigation with a potential terrorism nexus, investigators should notify both the bomb squad and the hazardous materials unit in their jurisdiction.

NOTES

Special Research Reports by ROCIC Publications

Accessible to RISS member agencies on the ROCIC secure Intranet website

- Internet Fraud: Techniques Used to Scam Online Consumers
- DXM: Teens Abusing Cough Medicine Risk Brain Damage, Death
- RISS Activity Report for G-8 Summit
- Mail Center Security
- Safety & Security for Electrical Infrastructure: Protecting Law Enforcement and the Public in Emergency Situations
- Crisis Response Report: Terrorist Attacks & Natural Disasters
- Eco Terrorism: Extremists Pose Domestic Threat
- Cold Case Units: Turning up the Heat
- Gypsies and Travelers
- User's Guide to ATIX: Anti-Terrorism Information Exchange
- DNA: Law Enforcement's New Investigative Tool
- False ID: National Security Threat
- Salvia Divinorum: Herbal Hallucinogen Raises Law Enforcement Concerns
- Smallpox: The Deadly Virus
- Human Trafficking: International Criminal Trade in Modern Slavery
- Network Security: Safeguarding Systems Against the Latest Threats
- Dirty Bombs: Radiological Dispersion Devices
- Ethics in Law Enforcement
- Law Enforcement Officers and Safety
- Computer Forensics: Following the Electronic Trail
- Huffing: Teens Abusing Inhalants
- RISSLeads Bulletin Board: Information in an Instant
- Bioterrorism
- Criminal Intelligence: Its Use in Law Enforcement in Our Changing World
- Terrorism: Defending the Homeland
- Law Enforcement and the Mentally Ill
- Civil Disorder: Preparing for the Worst
- Ecstasy: Harmless Party Drug Or Dangerous Trend?
- Heroin: More Purity For Less Money
- OxyContin Abuse Explodes In Southeast
- Just Say NO To Telemarketers
- School Security Crisis Response Manual
- XML: Communications Through Connectivity
- Credit Card Security Features
- Stop Phone Cramming: Check Your Phone Bill
- Shaken Baby Syndrome: What To Look For, What To Do
- Children and Internet Safety
- ROCIC's Illicit Drug Pricing: A Regional Comparison
- RAVES: When It's More Than A Party
- Identity Theft: From Low Tech to High Tech
- Hoaxes and Legends: How to Detect Hoaxes on the Internet
- Truce or Consequences: Motorcycle Gangs Talking to Each Other
- Child Pornography: Protecting the Innocent
- Meth Threat: Seizure of Labs by Untrained Personnel Recipe for Death and Destruction
- Illusion and Confusion: The Crime and Culture of Irish Travelers
- Date Rape Drugs: Rohypnol, GHB Gaining Popularity in Southeast, Southwest
- Security Threat Groups in Prison

ROCIC has been serving its criminal justice members since 1973, and served as the prototype for the modern RISS (Regional Information Sharing Systems) Centers.

ROCIC serves more than 180,000 sworn personnel in 1,727 criminal justice agencies located in 14 southeastern and southwestern states, Puerto Rico, and the U.S. Virgin Islands.

ROCIC provides a variety of services, free of charge, to its criminal justice member agencies:

- Centralized law enforcement databases with connectivity among law enforcement agencies and the RISS Centers using the RISS Nationwide Intelligence Network.
- Analytical processing of criminal intelligence, including phone tolls and document sorts
- Loaning of specialized, high-tech surveillance equipment and vehicles
- Publications, including criminal intelligence bulletin
- Specialized training and membership & information exchange
- Use of investigative funds
- On-site personal assistance by field service coordinators