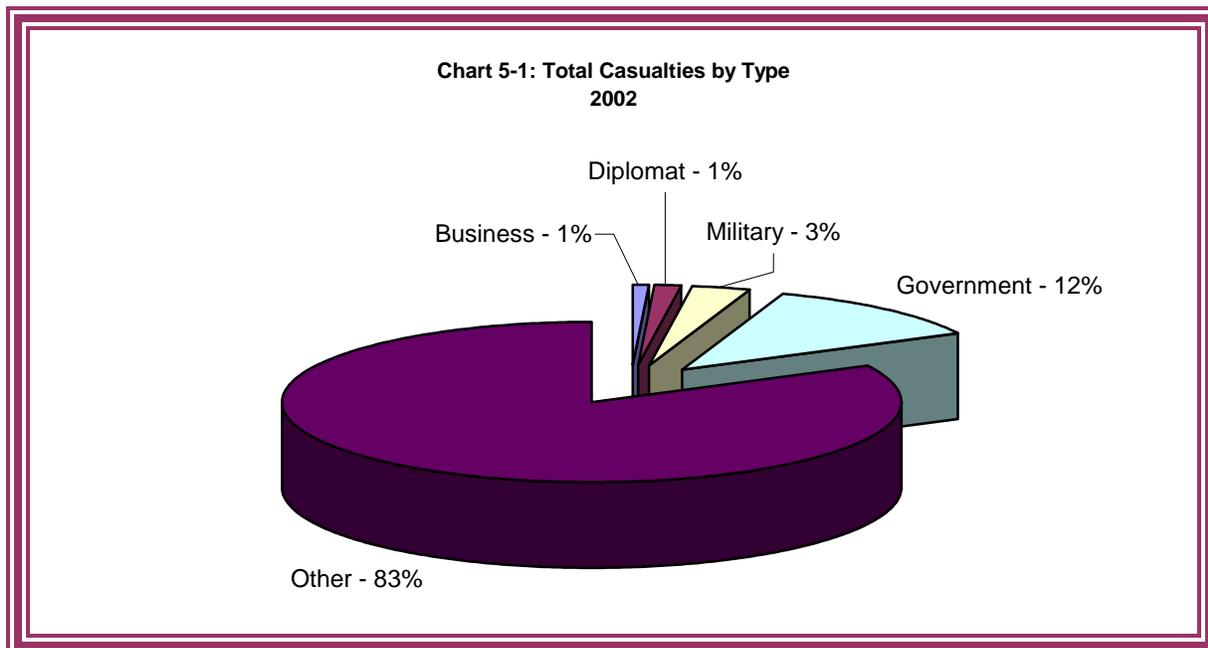


Chapter 5

The Terrorist Threat to U.S. Forces

This chapter will examine the threats to U.S. military forces. It is intended to provide the unit leader or planner with the likely terrorist actions confronting his or her unit. It is neither a region specific intelligence product nor an exhaustive list of terrorist scenarios, but a description of what techniques have been used against U.S. forces in particular situations, and what can be anticipated from trends in terrorist activities.

Reviewing the casualties resulting from terrorist operations in 2002, the military accounted for 3% of the worldwide figures. Although this is relatively small compared to the large number of casualties in the “Other” category (primarily civilians), Chart 5-1 demonstrates that government targets, which include the military, are definite objectives of terrorist attacks. Further, despite only one attack directed at a military facility, versus fourteen at diplomatic targets, military casualties exceeded diplomatic casualties by over two-to one.⁹² This indicates a significantly higher casualty rate per attack for military targets.



Section I: Categories of U.S. Forces

In discussing the likelihood of particular threats, it is necessary to make some differentiation between various types of units. For this guide, it is a simple classification according to the status of the unit as a deployed asset, deployable (or preparing to deploy) unit, or an activity or organization that does not deploy. This allows any unit to readily identify itself by its status. This system of division has been selected for its clarity, ease of use, and because terrorist targeting

⁹² Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2002* (Washington, D.C., April 2003), xx.

will be more concerned about where a formation is, who comprises it, and what it is doing, rather than what its' ostensible military function is. Sections II through IV will discuss each situation in detail.

Deployed

This category consists of units that are deployed to locations other than their permanent base. Units that are normally stationed in Germany or Korea do not fit in this category, because although they are overseas, they are based in those countries, and have the infrastructure and local familiarity that would accrue to a unit located at its CONUS base.

Deployed units are assumed to be operating away from their permanent bases, on either operational or training missions in overseas environments. This category includes named contingency operations, fixed rotations into stability operations, and training assistance to foreign militaries. It is not intended to address individual assignments to overseas locations such as attaches or foreign study immersion students.

Deployable

These are units that are either preparing for or in the process of deployment operations. It includes active component units within CONUS or permanently based overseas, even if not currently identified for movement, and reserve component units that are identified for named operations or notified for mobilization.

Non-Deployable

These are active component garrisons, training and logistic facilities, and other activities and installations that do not deploy. It also includes reserve component units and support activities not scheduled for deployment, but are conducting scheduled training drills and activities.

Section II: Terrorist Threat to Deployed Forces

In considering the threats to deployed forces, we will describe the relationship of terrorist action to various environments deployed units will operate in. We will also cover the general conditions that deployed units experience versus a terrorist threat. We will then look, in descending order of likelihood, at the primary threats expected to deployed units, the potential threats, and the possible threats. These will not be expressed in terms of actual terrorist groups, but in terms of likely tactics and approaches to be used by any group against deployed U.S. forces. Finally, we provide a short description of defensive and deterrent measures.

Environments and Conditions

Terrorists prefer to function in environments that reinforce their strengths and negate enemy advantages. They will want to maintain secrecy while discovering enemy information, focus on their objective while denying the enemy a concentration to strike, and achieve surprise. In most cases urban terrain favors the terrorist in accomplishing these ends. Cities provide the terrorist

with a population to conceal personnel, structures and facilities to hide and store equipment or weapons, and transportation nodes for movement.

Terrorists also prefer an environment that is chaotic, but not actually hostile. A fluid, poorly policed and uncontrolled situation permits suspicious activities to go unnoticed. However, terrorists prefer that the environment is not completely or continuously hostile. A hostile environment puts military forces on their guard, reduces the opportunities to get close to targets without being challenged or detained, and increases the difficulty of achieving surprise.

Terrorist groups will avoid operating as terrorists in an actual combat environment, because doing so negates their advantages, and allows conventional military strengths to be brought to bear against them. These strengths include such capabilities as battlefield intelligence and detection systems, high firepower, and reduced legal constraints on the use of force and the authority to arrest and detain, such as martial law or some variation thereof. Since civilians will normally try to escape areas of imminent combat, terrorists also surrender the advantages of surprise and security that hiding within a population brings them. Terrorists will sometimes forego their terror operations and operate as guerillas in areas of active combat operations. However, they may have to reorganize and equip for such operations.

The Impact of Martial Law – The Battle of Algiers

In the post-WWII surge of nationalist insurrections, the most notorious use of military authority to combat terrorism was the campaign waged by the French 10th Colonial Parachute Division against the urban terrorists of the Algerian insurgent movement FLN in the capital city of Algiers.

Algeria was one of the French colonies expecting to gain increased local rule, or perhaps independence, in the aftermath of WWII. When this did not occur, a nationalist insurgency began. By 1957 the nationalist groups, particularly the FLN, had been successfully carrying out a campaign of intimidation and terror that they felt would drive the French out of Algeria. The French responded by allowing the Army, in the person of General Massu and his *paras*, to employ legalized barbarity against the FLN and suspected sympathizers. This included torture, mutilation, and murder.

The resulting campaign of terror and counter-terror has become known as the “Battle of Algiers”, as much of the activity was initially concentrated in the capital city. While the French military scored significant successes, and broke the terrorist and guerilla forces in battle, they lost the war. Political support for the brutal suppression of the Algerians was eventually lost which directly contributed to the fall of the French constitution. After two attempted coups by French colonists in Algeria fearing that the mother country was giving in, France finally granted Algerian independence in 1962.

Likewise, deployed military forces will operate in one of two general environments: Base camps or tactical (field). Base camps are characterized by fixed facilities, either constructed or requisitioned, to provide shelter, support, and defensive capabilities to the units operating from them. Tactical environments are considered to be those where the unit operates with only organic support in the field, with no fixed facilities other than what the unit can improvise or what structures happen to be on the terrain.

This may appear to be a difference that has no impact, but in fact from the terrorist perspective, the differences are acute. Operating in a tactical environment means the unit might move at a moment’s notice in response to orders or necessities that the terrorist cannot anticipate. Base camps provide a much more stable and predictable target for terrorist planning. It is worthwhile

to note that of the terrorist attacks carried out on U.S. units deployed for operational and training missions, the significant casualties that were produced in Beirut and Dharhan (Khobar Towers) were in fixed billeting areas attacked by “purpose built” vehicle-borne improvised explosive devices (VBIEDs). Units in tactical conditions have experienced casualties from gunfire but nothing comparable to the destruction dealt to the fixed facilities.

It is important to note that deployed forces have some advantages that can contribute to their being less likely to be targeted for terrorist operations. These are:

- They are typically in a significantly enhanced force protection posture. Higher levels of alertness, control of approaches and access routes, and implementation of defensive measures reduce the likelihood of terrorist success, increase the costs to an attacker, and mitigate damage from successful attacks.
- They conduct appropriate planning and training to defeat or control hostile action. While this preparation may not specifically address terrorism, it does increase the probability of effective defense against attack, and reduces the casualties and damage if an attack should occur.
- Deployed units typically have increased access to intelligence assets and products. This information increases the effectiveness of the unit’s own intelligence, counter-intelligence, and force protection efforts.

Primary Threats

The primary threats to deployed forces will come from existing in-theater terrorist groups. This will often be in response to the U.S. military presence itself, or will constitute an attempt to influence U.S. policies regarding the use of military force. These terrorist groups will try to minimize their movement of personnel and equipment into the area of operations after the arrival of U.S. forces to avoid detection. Consequently, whenever possible they will attempt to pre-position operational assets. If they do need to position personnel or equipment in the area, they will do so employing all possible caution to avoid exposure to U.S. intelligence collection.



Figure 5-1: Khobar Towers Dhahran, Saudi Arabia, 1996 (Source: DOD Photo)

The most dangerous form of attack historically used against deployed U.S. forces is the large vehicle-borne improvised explosive device (VBIED). This tactic has been used primarily against units in a base camp environment. The setback and protection common to deployed unit perimeters requires a large and effective weapon to produce the large number of casualties the terrorists want to achieve. Consequently, the delivery of adequate explosive weight to overcome this setback and layered security requires a

vehicle. VBIEDs equaling thousands of pounds of explosive power can produce the blast wave and secondary missile effect needed to cross the intervening space and still cause damage. The Khobar Towers VBIED was estimated to be the explosive equivalent of 20,000 pounds of TNT.⁹³ Table E-2 in Appendix E has a DOD chart that details the various size explosive devices with their comparable evacuation distances to avoid casualties.

While possible that a unit in a field environment would be attacked by a large VBIED, it is much less likely. The preparation and deployment of such a weapon requires time that would likely be wasted if the target unit moved or improved its positions. This does not rule out the use of smaller weapons with faster preparation cycles if they can be effectively delivered and detonated. Obvious lapses in security procedures, insufficient setback of personnel and facilities from the perimeter, or habitually assembling units (convoys, patrols, road marches, etc.) in unsecured locations outside perimeters are instances where smaller explosive devices can be effective.

Delivering either a large or small explosive device by means of a suicide asset may or may not increase the effectiveness of such a weapon. If the vehicle checkpoint and barrier system is 800 meters from the target, and there is a perimeter fence or wall 400 meters from the target, why bother ramming the gate with a suicide operator? Parking the device next to the perimeter fence and leisurely setting the fuse and retiring will be more effective than expending a suicide asset that will likely have to detonate twice as far from the target.

The attack on the Marine Corps barracks in Beirut is a different case. The suicide driver breached the gate and delivered the VBIED directly to the target. In this case the use of a suicide bomber increased the effectiveness of the attack. Conversely, at Khobar Towers, the vehicle access point was not considered breachable, and it was anticipated that any VBIED would be detected. Therefore a point was selected on the perimeter closest to the target at which to park the weapon, and a suicide operator rendered unnecessary.

Attacks have been used to defeat specific perimeter security positions (dug-in heavy weapons) with one suicide asset in the first assault, and then followed up with a second suicide asset accompanied by an assault team with supporting fire from overwatch positions to destroy a key target concentration within the perimeter.⁹⁴ Because of the value of suicide assets, though, this is an expensive tactic. However, it must be considered in planning in areas where the use of suicide attacks is possible.

The most common form of attack used against deployed forces is the light weapons ambush, involving grenades, small arms, light bombs, and rocket launchers.⁹⁵ Additionally, IEDs are being used more in these type attacks. The targets of these attacks are likely to be fixed positions engaged from a moving vehicle, or small units on the move engaged from vehicles or stationary positions with adequate escape routes. This is a considerably less effective casualty producing tactic than the VBIED, as it pits itself against the strengths of a tactical unit, and is the sort of

⁹³ Department of Defense, *Report on Personal Accountability for Force Protection at Khobar Towers*, by William S. Cohen, (Washington, D.C., July 31, 1997), 2.

⁹⁴ Rohan Gunaratna, "Suicide Terrorism in Sri Lanka and India," in *Countering Suicide Terrorism* (Herzliya, Israel: Interdisciplinary Center Projects Publishing House, 2002), 107.

⁹⁵ Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 160.

attack most of the U.S. military draws its pay to anticipate, identify and defeat. It also carries the least psychological impact, as most people rightly view firefights of this nature as part of the military mission. Despite this, these attacks have successfully caused U.S. military casualties and drawn international media coverage. They are the easiest and quickest type of attack to plan and stage, and therefore have a high probability of use by a terrorist threat, especially against tactical formations in the field.

The light weapons type of attack described above may be deliberately launched from a group of civilians. This provides concealment for the terrorist(s), as well as complicating the defensive reaction. Engaging the attacker when shielded by non-combatant bodies will almost certainly result in civilian casualties, which can then be exploited by the terrorists for their publicity and propaganda value. On the other hand, if the U.S. forces attempt to apprehend or neutralize the attacker without inflicting collateral non-combatant casualties, the U.S. action may be ineffective and expose the force to other attackers concealed within the group anticipating the U.S. attempt to limit civilian casualties.

In assessing the terrorist threat to a deployed force in a particular area of operations, the effectiveness of poorly resourced local groups should not be underestimated. Low to mid-capability groups motivated the removal of U.S. forces from areas such as Beirut and Somalia in the past (while Somalia was not the result of planned terrorist action, the exploitation of the casualties and psychological impact from the failed U.S. mission are classic terrorist media techniques). While actors from outside the immediate area of operations supported our adversaries in both these incidents, the operations themselves were executed locally. Further, the prestige associated with successfully challenging U.S. forces brings benefits to the groups involved through increased support and positive perceptions by the local populace. These positive results then become incentives for further attacks.

Potential Threats

Less likely than attacks by the existing in-theater groups are attacks by organizations that cannot otherwise reach U.S. targets either in CONUS or in other overseas areas. These groups will take the opportunity to attack U.S. military forces exposed in a third country. This can happen even if the U.S. forces are not a direct threat to the terrorist group, or are not conducting activities that are “objectionable” to the terrorists. The terrorists’ attraction to the opportunity target of U.S. forces in a country that is a “permissive environment” is obvious. Such a country would be one with poor border control, a weak or unstable government, and easy access to weapons or smuggling routes. A successful attack could be exploited for objectives unrelated to the actual U.S. military mission.

In these circumstances the target of the attack may be more symbolic in nature, striking at significant individuals occupying positions of power or influence. Targeting senior commanders, particularly while in transit to or from a deployed unit in a permissive or exposed environment has been a frequent objective of terrorists. Attempted assassinations of key unit personnel should be considered a distinct possibility, with any number of methods available to the terrorist (see Appendix C for a discussion of assassination operations).

An example of this sort of “target of opportunity“ operation was the bombing of the USS *Cole* in Aden harbor in October of 2000.⁹⁶ While the presence of the USS *Cole* was unwelcome to the fundamental Islamics that carried out the attack, the situation exposing the ship to terrorist action in that environment was an irresistible opportunity. The USS *Cole* was no direct threat to terrorist organizations ashore, and the refueling operation conducted in Aden was specifically meant to be unobtrusive to local sensibilities. However, the vulnerability of the ship indicated a high probability of success against an obvious symbol of the United States. The resulting casualties and images of the damaged warship were exactly the result the terrorists were looking to achieve.



Figure 5-2: Suicide Bomb Damage to USS *Cole*. October 2000
(Source: U.S. Navy Photo)

The USS *Cole* bombing used another VBIED, the vehicle in this case being a boat. Deployed forces should not ignore the possibility of explosive devices or other attack methods being delivered by boat or air. The Tamil Tigers (LTTE) used suicide and remote-controlled explosive motorboats against Sri Lankan government targets. Various groups employed ultralight aircraft, powered and unpowered hang gliders, small civilian aircraft, and remote control aircraft to deliver attack teams, explosives, or suicide bombers to particular targets.⁹⁷ A unit that successfully interdicts or controls all surface approaches should not neglect the possibility of an aerial approach. Nor should a unit exposed to a waterborne approach assume that control of surface approaches is sufficient. Several terrorist groups have successfully utilized divers in underwater infiltrations and attacks.

A potential threat that has been employed against other nations’ military forces with some success is the capture or kidnap of small units or individuals on missions that isolate them from the larger unit. The individual soldiers may be used as hostages, tortured, or killed for psychological effect. U.S. prisoners of war found themselves used as human shields, hostages, and worse in previous conventional conflicts. Individual U.S. government and military personnel have been kidnapped and exploited by terrorists when serving on individual missions overseas. The uses of “atrocious videos”, such as showing the torture and murder of prisoners in the Balkan, Algerian, and Afghan (Soviet) conflicts, are becoming common practice among terrorist

⁹⁶ John McWethy et al., no title, *ABCNews.Com*, (18 October 2000); available from <http://www.abcnews.go.com/sections/world/DailyNews/cole001018b.html>; Internet; accessed 9 January 2003.

⁹⁷ Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 165.

organizations to attract and indoctrinate recruits, and terrify the opposition.⁹⁸ The proliferation of this type of imagery indicates a clear inclination to exploit captured personnel for terror effect.

Possible Threats

Other possible threats include provocations by external or internal politically affiliated terrorist groups to induce U.S. action to achieve a desired outcome. In the Balkans, for example, the various ethnic and religious factions continually attempt to blame each other for harassment, graffiti, arson, and drive-by shootings. In fact, some groups would carry out incidents against their own property and people, and attempt to implicate their opponents to provide a suitable cause for SFOR (Stabilization Force) involvement.⁹⁹ Their goal was to provoke SFOR into suppressive action against their enemies.

Another potential threat is the possibility of punitive attacks against family members of forward deployed personnel. This could be either retaliation for actions taken by U.S. forces, or a preemptive action designed to lower morale and decrease unit effectiveness. It could also

Family Matters – Reprisal Attack after The USS Vincennes Incident
Navy Captain Will Rogers commanded the USS *Vincennes*. In the summer of 1988, the *Vincennes* shot down an Iranian airliner that the ship misidentified as an Iranian fighter. Rogers' wife Sharon was targeted in a terrorist attack eight months later on 10 March 1989 in San Diego, California. The car she was driving was destroyed by a pipe bomb, but she was unharmed. While this example deals with a higher profile incident than most deployed unit members and family would face, the threat is clearly there.

Source: www.sandiego-online.com/retro/setpretro2.stm, Internet, accessed on 1/14/03

be intended to provoke reprisals by U.S. soldiers against civilians in the area of operations.

Such attacks would depend upon the operational reach of the terrorist adversary, or their ability to engage a proxy organization to conduct such an operation for them. If actual attacks are impractical, threatening messages directed at family members could be employed to erode soldier confidence and morale. Falsified emergency notifications and Red Cross messages could be employed to the same effect.

Preventative Measures

**"Expect only 5% of an intelligence report to be accurate. The trick of a good commander is to isolate the 5%."
- General Douglas MacArthur**

The greatest deterrent to terrorist action is aggressive OPSEC programs emphasizing surveillance detection and counter-intelligence activities. While physical security measures are essential, they can be neutralized or avoided by terrorists with adequate preparation. Terrorists

⁹⁸ Jason Burke, "You Have to Kill in the Name of Allah until You are Killed," *Guardian Unlimited* (Observer Special Report, 27 January 2002), 3; available from <http://www.observer.co.uk/islam/story/0.1442.640288.00.html>; Internet; accessed 15 January 2003.

⁹⁹ Department of Defense, *11th Psychological Operations Task Force After Action Report for SFOR X*, by MAJ Clint A. Venekamp, (Upper Marboro, MD, July 2002).

must have superior target intelligence to select targets, circumvent security, and plan operations. Deny them this information, and they cannot operate effectively. Detecting them collecting target data permits anticipation of possible terrorist courses of action.

Information the deployed unit should consider obtaining includes any record of surveillance incidents directed against U.S. diplomatic or commercial activities in the country. Correlation of confirmed surveillance against these potential targets permits a deployed unit to identify personnel, vehicles and techniques in use in that area prior to arrival. Terrorists have the capability to use sophisticated tradecraft that will complicate this correlation, but they have also been known to use the same personnel and vehicle repeatedly in surveillance tasks. The Khobar Towers pre-attack surveillance was conducted using one vehicle for all surveillance missions. That vehicle was observed and reported 10 times out of 40 separate uses as a surveillance platform.¹⁰⁰ The only reason this was not fatal to the attack plans was that nothing was done to correlate and interpret this information by U.S. forces.

Unit planners should seek out any record of actual terrorist activities in the area, whether directed against U.S. interests or not, from intelligence, security and law enforcement sources. Additionally, groups or individuals considered dormant or inactive should be reviewed based upon the possible change in attitude or motivation that a U.S. deployment into the area might cause.

Variation of a unit's operational patterns is a basic but useful technique to deter attacks. It prevents anticipation of target actions by the terrorist(s); it introduces uncertainty to his planning, and sharpens the alertness and observations of unit personnel by avoiding routine. Terrorist operations have been called off, and attacks in progress have been "blown" due to simple changes in the routine or activity of a target.

This is by no means an exhaustive list of threats to deployed U.S. forces. Intelligence specific to the area of operations must be studied and integrated into realistic threat assessments for deployed units. However, terrorists have used the techniques mentioned in the scenarios discussed here multiple times against deployed military forces. These techniques will continue to be employed by terrorists in modified forms with innovations in weapons or tactics as long as they continue to be effective.

Section III: Terrorist Threat to Deployable Forces

In this section we will discuss likely threats to U.S. forces in the deployable category. "Deployable forces" are considered to be those units that are either preparing for or in the process of deployment overseas. It includes active component units both within CONUS and permanently based overseas, (even if not currently identified for movement) and reserve component units that are identified for named operations or notified for mobilization. The purpose for identifying "deployable" units in this manner allows us to consider possible threats to a unit ranging from their home station to their debarkation point during a deployment.

¹⁰⁰ Department of State, Bureau of Diplomatic Security, *State Department Diplomatic Security Surveillance Detection Program Course of Instruction* [CD-ROM], (Washington, D.C., October 1999).

Additionally, this category addresses those threats directed at war fighting or operational units not immediately slated for movement. Installations will be discussed in Section IV.

Reserve component units identified for mobilization or participation in named operations fall into this category even though their deployment may not be imminent. This is because of the increase in training activity and resources they receive, as well as the possibility that their participation in a particular operation will motivate an attack. When discussing home station activities, we will also consider attacks launched against off-duty personnel known to be military, and targeted because of that fact.

This section will be organized like Section II, discussing primary threats, potential threats, and possible threats to deployable forces. It will be broken down further to address threats during normal home station activities, and threats during actual deployment activities. A separate subsection will address special considerations in the case of units whose home base is overseas. Finally, we will briefly outline some applicable preventative measures.

Primary Threats

The most likely threats to deployable U.S. forces either at home station or during deployment will be from terrorists external to the U.S. These organizations will be international or transnational groups with either an operational presence already in the U.S. or support infrastructure in place to facilitate the arrival of operational assets. They quite possibly will be state sponsored organizations, or organizations operating for profit or for other material considerations on behalf of some government. In some cases they could be state intelligence or covert military special operations forces. While in raw numbers of incidents, domestic terror groups were responsible for more attacks and attempted attacks on U.S. military targets than external groups in the past, most of these attacks were on facilities and installations, not units and personnel.

However, state sponsors or transnational terror groups may also use domestic groups that can be exploited through shared ideology or for profit considerations to conduct operations in the U.S. against military targets. The El Rukns group, a Chicago based gang, negotiated with Libya to attack a domestic airliner with a surface to air missile in 1985.¹⁰¹ Since Libya directed and sponsored lethal attacks by the Japanese Red Army on U.S. military targets in CONUS and abroad during the same period of time¹⁰², there is little doubt that Libya would have utilized a domestic U.S. group had one been available and capable. There is also evidence indicating that al Qaeda is subcontracting to like-minded terrorist groups to conduct operations.

Home Station Threats

Threats to deployable units at their home station during pre-deployment activities will most likely consist of attacks on units conducting movement to or from training activities, and attacks

¹⁰¹ Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 162.

¹⁰² Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 188-189. The JRA adopted the name "Anti-Imperialist International Brigades" for these operations.

upon off duty personnel during social gatherings. The intent would be to demonstrate the capability to damage U.S. military forces, and weaken morale. The most likely methods of attack would be a small to medium size improvised explosive device (IED), or an ambush conducted with light weapons (automatic weapons, grenades, and anti-tank rockets).

Attacks on units training will most likely take place during movement because:

- The unit is concentrated during movement, and typically dispersed during training.
- Training areas are usually harder to access by non-military personnel than roads leading to or from them.
- Units training have a greater degree of alertness than units in an administrative road movement.
- Units conducting training have greater self-defense capabilities, especially if they are training with live ammunition.
- Routes to and from training areas are well established, almost habitual, whereas movement during training is more difficult to pattern.

Attacks on personnel at social gatherings can occur at clubs on post, or during unit functions at private homes or commercial establishments off post. Traditional observances of organizational days (Army Birthday, division or regimental days) are often publicized in advance and give attackers planning dates for possible gatherings in accessible locations. Attacks at commercial entertainment establishments such as bars, clubs and restaurants off post are less likely because the density of military personnel at a particular establishment is usually not sufficient to gain the appropriate impact (off-post establishment attacks are addressed under the Section “Units Based Overseas”). The most likely attack method will be a small to medium sized IED, although terrorists may employ improvised mortars or other standoff weapons.

Deployment Preparation and Movement

Attacks on deployable units are likely to occur during actual preparation for deployment activities. The specific mission may inspire an attack by a group who wishes to prevent the deployment, or a potential adversary may attempt to extend the depth of the battlefield by engaging units with unconventional terrorist attacks before they arrive in theater. Objectives of these attacks will depend on the mission of the deploying unit and the context of the mobilization, but may include:

- To delay or prevent mobilization or deployment.
- To render the unit non-mission capable for deployment.
- To decrease unit effectiveness when deployed.

Delay or prevent mobilization or deployment.

Operations aimed at this objective would involve either disrupting the unit enough to prevent its movement on schedule, or disrupting the transportation cycle for the unit. Disruptions sufficient to prevent the unit from making movement would probably also render it non-mission capable for deployment. This will be covered in that sub-section below.

Disruption of transportation may take place by sabotage or direct attack upon the unit being transported and its conveyance. Methods of attack would be selected depending upon their effectiveness versus the mode of unit transport. Air, rail and sea are the modes of transport for long voyages, but frequently units must use ground conveyances such as buses or organic vehicles to get to their embarkation point. Consequently, attacks may also occur against these vehicular movements. Weapons likely to be employed include bombs, AT rockets, and potentially, guided missiles. If sabotage is used in preference to direct attack, the sabotage will be designed to produce maximum casualties in the ensuing crash, derailment, fire, etc.

Based upon the availability of military air transport, the deploying unit may be required to move via commercial or chartered air. Since movement from home station to the mobilization station or embarkation point may not originate near a large military airfield, the unit may need to use a civilian airfield, even if military air is available. Civilian fields and chartered aircraft present terrorists with opportunities for attacks unavailable against military aircraft flying from military airfields. This was demonstrated in January 2003 when intelligence sources detected the targeting of chartered aircraft participating in the build up of forces against Iraq.¹⁰³

Despite the emphasis on the vulnerabilities of airlift, all forms of transport are subject to sabotage or attack. Domestic terrorists have derailed U.S. passenger and cargo trains¹⁰⁴, and attacks on ships in port and at sea are well within the capabilities of most transnational and international terror groups.

Destroying facilities such as docks, airfields, refueling facilities, and cargo terminals at intermediate stops or at the final destination is another way for terrorists to prevent or delay deployment. It is a method of adding depth to the battlefield during a conflict, and does not require the projection of assets and weapons into more distant countries. If timed to coincide with the arrival of incoming units, such destructive attacks could cause significant casualties.

Render the unit non-mission capable for deployment.

The objective here is to cause sufficient damage or disruption to the unit so that it will be unable to deploy, or will be unable to function once deployed. The most direct way to do this is to inflict casualties on the unit. IEDs, rocket launchers, and mortars directed at unit assemblies such as formations, manifest calls, and other pre-deployment personnel concentrations are the most

¹⁰³ Thom Shanker, "Officials Reveal Threat to Troops Deploying to Gulf," *New York Times*, 13 January 2003; available from <http://www.nytimes.com/2003/01/13/politics/13INTE.html>; Internet; accessed 13 January 2003.

¹⁰⁴ Jim Hill, "Sabotage Suspected in 'Terrorist' Derailment," *CNN.com*, 10 October 1995; available from <http://www.cnn.com/US/9510/amtrak/10-10/>; Internet; accessed 15 January 2003.

likely scenario. A terrorist group with a rudimentary biological weapons capability could infect enough of a unit with a contagious disease that it would have to undergo quarantine, delaying deployment. This is a less likely and somewhat uncertain proposal from the terrorist point of view, but might be used to bypass defenses designed to prevent other forms of attack.

Another possibility to consider is the destruction of a key piece of equipment or the assassination of key personnel. This is less attractive to the terrorists because they cannot be sure that such losses would not be rapidly replaced. Unless the terrorist group is aware of specific personnel or equipment shortages, they will rely on the more certain method of mass casualties.

Decrease unit effectiveness when deployed.

This objective requires actions to undermine morale and destroy unit efficiency. It will be characterized by less lethal, more harassing activities. Contaminating unit equipment with low level radiation sources, infecting unit information processing equipment with viruses, harassing or attacking soldiers' family members, and inserting false messages of death or illness into the various notification systems to both family and service members are all possible scenarios. With the exception of actual attacks on service members' families, these activities do not require significant operational skill or resources.

Potential Threats

Home Station Threats

Although less likely than transnational or international terrorists attacks, domestic groups who object to U.S. military involvement overseas, or to the political goals of U.S. policy still have potential to conduct attacks. Such groups would share the objectives listed above, with the further aim of publicizing the domestic dissent to the particular mission or policy. Such groups could develop capabilities very rapidly, and coalesce from existing organizations with ostensible "anti-capitalist/imperialist" ideologies. Although they are nearer to the targets and less visible to casual suspicions than foreign personnel, domestic terrorists would be constrained in conducting significant lethal attacks due to the possibility of severe backlash for actions against fellow citizens.¹⁰⁵ Actions would probably start out with symbolic and non-lethal arson, vandalism, and sabotage. If these fail to ignite public support for the terrorists' goals, their organizations would increase in radicalization, and attacks would become more lethal, as happened in the Vietnam-era anti-war movement.¹⁰⁶

There is also the potential for domestic groups to attempt to obtain advanced military technology or new equipment by raiding units during normal training activities. This threat is most likely to come from groups who wish to rapidly increase their offensive capabilities in anticipation of paramilitary operations. Groups whose ideology emphasizes insurrection, social warfare, or "local" uprisings are most likely to attempt this type action. It is likely to be directed at National Guard and Reserve facilities (See Section IV).

¹⁰⁵ Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 94.

¹⁰⁶ *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Student Terror: The Weathermen"

Deployment Preparation and Movement

As discussed above, domestic groups who object to U.S. military activity or U.S. policy could conduct operations against deploying units. A key difference here is that attacks of this nature would probably start out at the lethal end of the spectrum. Either because the domestic groups are conducting operations sponsored or directed by external actors, such as other terrorist groups or nations, or because imminent deployment would increase the sense of radicalization of these groups. Such groups would share the objectives for preventing or delaying unit movements discussed under “Probable Threats”, with the further aim of using such actions to publicize their dissent.

A particular specialty of domestic groups is their capability to conduct harassment campaigns against individuals peripherally associated with or employed by activities these groups object to. Such a campaign undertaken by a domestic group against service members’ families with the objective to reduce unit morale and effectiveness would be extremely disruptive. Harassment campaigns have included lethal and near lethal attacks, as well as disrupting the victim’s daily life and instilling constant, pervasive fear in the victim. Such a campaign added to the normal stresses associated to military careers and deployments could have extremely negative consequences in both the long and short term.

Possible Threats

Possible threats to both home station activities and deployment activities could come from U.S. resident aliens or citizens not specifically organized or affiliated with larger terrorist networks. These groups may have loyalties to ethnic, religious, or nationalist causes hostile to the U.S. or opposed to U.S. policies. Expatriate and immigrant ethnic groups threatened action against government and military targets in the U.S. and Europe when SFOR activities or policies in Bosnia-Herzegovina were perceived as contrary to the best interest of their ethnic “home” state or group. Other immigrant and expatriate groups have provided support for various hostile activities directed against particular U.S. foreign policies. While largely unorganized, even individuals with little support but high motivation can have major impacts. Jordanian Sirhan Bishara Sirhan assassinated Senator Robert Kennedy in 1968 because of his assumption that Kennedy would likely be the next U.S. President, and he wished to prevent Kennedy’s expected support for Israel.

Units Based Overseas

Units based in overseas locations have several special considerations. Because of different conditions in OCONUS locations, their home station routine is more vulnerable to terrorist attack than similar units based in CONUS. Europe is an excellent example where attacks on U.S. service members have been extensive and lethal.¹⁰⁷ Some attacks were state sponsored or directed, which made them even more dangerous.¹⁰⁸

¹⁰⁷ *International Encyclopedia of Terrorism*, 1997 ed., s.v. “Chronology of Terrorist Events.”

¹⁰⁸ Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 71.

There are two principal conditions contributing to the higher level of threat to overseas-based units. The first is exposure. Countries that have permissive border controls, countries that are located closer to states that harbor or sponsor terrorists, or that have active terrorist groups within their borders, all increase the ability of terrorists to reach U.S. military units and personnel based therein. This situation is best illustrated in Europe, where internal border control between European Union (EU) nations is no longer required. Once the borders of a EU member are penetrated, travel to all member countries becomes possible with minimal control. The proximity of the EU to states sponsoring terrorism is much greater than the U.S., and the smuggling and criminal trafficking routes used by terror groups pass through or close by EU nations. Additionally, several EU nations still have very capable terrorist organizations based within their borders.

The second condition is visibility. U.S. military personnel are usually highly visible in overseas environments, particularly in countries that emphasize their homogeneity, such as Japan and Korea. This not only aids in targeting U.S. personnel; but also contributes to another kind of visibility - political visibility. U.S. military presence is frequently a contentious issue in local politics in host nations. This political visibility can lead to resentment of the U.S. presence, and ultimately to attacks against visible signs of that presence, such as military personnel.

The most common threat to overseas-based units is attacks directed against off-duty personnel, either at social gatherings or at entertainment establishments. This is different from the home station situation for CONUS based units because personnel overseas tend to cluster socially, frequenting particular establishments in large numbers. This density provides sufficient military victims for the terrorist attack to achieve the desired effect. Also, significant civilian casualties can be exploited as a wedge issue, to be driven between the host nation populace and the U.S. military. To the terrorists, causing civilian casualties at a club in an American town would simply be more dead Americans. Attempting to instill negative feelings toward the military in the local community would be nearly impossible. However, dead civilians from a host nation can be "blamed" on the U.S. presence by the terrorists, and can raise the question in the host nation political system of the costs of hosting foreigners who are going to attract political violence to their communities.

Other attacks that have been conducted against units based overseas have principally involved rocket launchers, improvised mortars, and bombs directed against key leaders and on-duty personnel. These attacks have ranged from the low end of sophistication to highly technical operations. While unlikely, the possible use of chemical or biological weapons should be acknowledged. The 1995 Tokyo subway nerve agent attack was conducted by the Aum Shinrikyo cult, which was (and is) virulently anti-American. Aum had a significant interest in all forms of WMDs, and in addition to the nerve agent Sarin, had several other types of chemical and biological weapons under development.¹⁰⁹ Aum's central philosophy focused on the inevitability of nuclear Armageddon, and the cult occasionally considered provoking such a conflict so they could fulfill their appointed role in such a disaster. Given more time, Aum might have effectively employed some of these chemical or biological weapons against U.S. forces in Japan.

¹⁰⁹ Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 125.

Vandalism, sabotage and arson attacks have also been used for symbolic effects, but are usually intended to be non-lethal. These types of actions can also occur during political demonstrations against U.S. military presence as a provocation to host government police or U.S. security personnel to further polarize attitudes.

Preventative Measures

As previously mentioned in Section II, denying terrorists the target information they require is the most certain deterrent. Unlike deployed units, deployable units will have installation security measures, functioning local law enforcement activities, and other non-military security and investigation organizations operating in their environment. Therefore the unit OPSEC, force protection, and security programs are not the sole reliable resources to the unit planner.

One place where unit training and knowledge can assist in denying the terrorist target information is in access control. Because units are stationed within functioning communities, there are many interactions with non-military individuals and activities. Since there are multiple jurisdictions involved, there are various legitimate permissions to access military posts. Unit personnel should be familiar with the various types of access control documents they will encounter. If required to establish or man access control points, unit leaders should become familiar with the capabilities of common counterfeiting technologies and their effectiveness in duplicating access control and identification documents. Due to advances in digital camera and image enhancement technology, loss or theft of documents is no longer necessary for reproduction. Likewise, electro-optical zoom lenses and hidden micro-cameras can gather keypad combinations and PIN numbers for security systems.¹¹⁰ Unit planners need to understand these new vulnerabilities in order to mitigate them where possible.

Deployable forces face a variety of threats, but most are relative to their role as war fighting organizations either preparing for or moving to their missions. Their value as a terrorist target is driven by policy decisions beyond their ability to affect and may be subject to attempts to expand potential conflicts to the U.S. homeland. Therefore anticipation and alertness are the most important factors in mitigating the threat.

Section IV: Terrorist Threat to Non-Deployable Forces

In this section we will discuss threats as applied to U.S. forces in the non-deployable category. Non-deployable forces consist of installations, fixed infrastructure, and training establishments. It also includes National Guard and Reserve units and facilities not currently listed for deployment. Since these activities are more or less permanently fixed, we will only consider the likely threats for the United States and its' territories. Also, since these activities provide the logistic and power projection capabilities for any deployment of U.S. forces, they are likely targets of terrorist groups.

¹¹⁰ Paul Kaihla, "Forging Terror," *Business 2.0* (December 2002): 3; available from <http://www.business2.com/articles/mag/0,1640,45486%7C5,00.html>; Internet; accessed 22 November 2002.

As in the previous two sections, we will again divide the threats according to likelihood, covering primary, potential, and possible threats. While deployable and deployed forces are particularly at risk during conflict or times of international tension, non-deployable forces will experience threats based upon domestic political tensions as well. These tensions could inspire action by a variety of social and single-issue domestic extremists from all sides of the political spectrum.

Primary Threats

The most probable threats to non-deployable forces of all kinds will likely be domestic groups with a variety of objectives. While the domestic terrorism landscape is cluttered with any number of ideological and religious motivations, most U.S. domestic terror groups have embraced the “leaderless resistance” model of organization. While this tends to limit the complexity and sophistication of these operations, it also reduces the effectiveness of infiltrating the group or developing informers, because of the decentralized nature of operations (See side bar).¹¹¹ As the Oklahoma City bombing conclusively showed, “simple” attacks do not equal “ineffective” or “non-lethal” attacks.

Certainly the greatest single threat in this category is the attack intended to obtain military weaponry or equipment.

In the 1970s alone, enough small arms were stolen from U.S. military facilities to outfit a force of approximately 8,000.¹¹² These operations are conducted by a variety of groups, but most recently groups associated with white supremacists, various “Christian Identity” offshoots, or the “militia” movement predominate in this area. They are conducted as “inside jobs” or theft more often than actual overt raids or attacks, but the capability and inclination for violent operations is there. If the terrorist group believes the objective warrants it, assault style robberies of military equipment will occur (See the example on the next page).

Another likely threat is that transnational or state sponsored groups could target key infrastructure or support installations to reduce the military’s power projection capabilities. This

Leaderless Resistance

Simply put, leaderless resistance involves individuals or extremely small groups (two or three persons) who share common goals and values with a larger whole. They remain unaware of each other, and rely upon themselves to conduct actions against the enemy. While it bears similarities to network style organizations, the lack of communications links between nodes makes it more like a mob or riot phenomenon. Everyone in it seems to know what to do collectively, with little communication.

There is usually an ideological center to such groups; an individual or cabal who sets the tone for the larger mass. This center remains unaware of the radical members and their intentions. They outline an ideal condition or future to be achieved, and then exhort their followers to obtain it, without going into specifics on the method to be employed. “You know what to do” is the mission order in this environment, allowing the “leader” to avoid incitement or conspiracy charges, while claiming credit for the work of the unknown individuals or cells.

¹¹¹ Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999*, Report 0308, (Washington, D.C., n.d.), 18.

¹¹² Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 111.

transnational presence was exhibited in 2002 when two suspected al Qaeda cells were neutralized; one in Portland, Oregon and another in Lackawanna, New York. Well-funded adversaries without a significant operational presence in the U.S., or who desire deniability, could instigate attacks utilizing various domestic groups as proxies. Money or common ideology or goals would provide the basis for this cooperation. This sort of attack would have slightly different objectives than those discussed in Section III. The destruction of critical logistics and transportation infrastructure such as rail lines, pipelines, and warehouses would emphasize arson and sabotage. Unfortunately, these capabilities are highly developed in most of the domestic U.S.

Domestic Threat To National Guard Armories

From “Terrorism in the United States, 1999” FBI Publication #0308, Federal Bureau of Investigation

On December 8, 1999, Donald Beauregard, Commander and Brigadier General of the Southeastern States Alliance (SSA) was arrested on six felony counts related to his plans to steal weapons and explosives from National Guard armories in central Florida, attack power lines in several states, and ambush federal law enforcement officers. The SSA was an “umbrella” organization composed of individuals from several militias in Florida, Georgia, South Carolina, Alabama, and other southern states. The objective of the now-defunct organization was to create social and political chaos, which members believed would cause the U.S. Government to declare martial law, thus inciting a popular uprising and violent overthrow of the Federal Government. The SSA theorized that Beauregard’s plan would create this chaos and further their goal of violent revolution. Beauregard was charged with violating several federal laws, including Title 18 USC Section 371, conspiracy to break into a military facility to steal weapons and explosives; Title 18 USC Section 2339, providing materials in support of a terrorist organization; and four counts relating to Title 26 USC, firearms violations—transferring a sawed-off shotgun, possession of a silencer, transfer of a firearm without a serial number, and manufacture of a sawed-off shotgun.

groups that could act as proxies for a hostile foreign entity.

Also, “softer” installations with a high concentration of military personnel and families could be attacked with mass casualty producing weapons for the pure terror and psychological impact on the military services as a whole. The uncertainty and personal devastation this would cause would be serious enough. However, the amount of resources that would have to be directed into countermeasures in order to restore soldier confidence and morale could degrade war fighting capabilities.

Another type of target that may be selected for the sheer morale and psychological impact is the highly symbolic target. The attack on the Pentagon in 2001 is an outstanding example of an attack with this objective. Another highly symbolic military target is Arlington National Cemetery adjacent to Fort Myer. Many other posts have less famous, but still symbolically significant monuments and activities that could be subject to attacks under this scenario.

Potential Threats

Conflicts over domestic social policies have a probability of causing attacks on military installations. While not participants in these policy debates, the U.S. military services have been

the instruments of major social reform at the direction of both Congress and the Executive Branch. The military services have led the nation in implementation of social policies such as complete integration of racial minorities and women. Groups on both sides of contentious social issues in U.S. domestic politics watch various proposals regarding military implementation of policies regarding their particular causes. Decisions by Congress for or against military implementation of social policies on contentious domestic issues could very likely spark violence by the more radical elements of either side in these debates. The capabilities of groups involved in these issues, and the level of violence already displayed against other segments of society involved in a variety of contentious social issues make this a significant concern.

The emergence of a radicalized, ostensibly “anti-war” movement is also a distinct possibility. This sort of “anti-war” movement does not need an actual conflict to be initiated. “Anti-war” rhetoric and agendas have been incorporated into large protest gatherings such as “The Battle of Seattle” (Seattle World Trade Organization meetings in 1999) prior to the terror attacks on the U.S. and the subsequent military retaliation. The recent shifting and redefining of the traditional “radical left” ideological focus to an anti-capitalist, anti-globalization, and “economic and social justice” agenda has made any military action by U.S. forces - whether the mission is humanitarian, disaster relief, or actual combat – suspect in their eyes. Many of the left wing and single-issue organizations that espouse the anti-capitalist, anti-globalization, and anti-war rhetoric are branches or offshoots of international organizations.¹¹³ These groups maintain ideological linkages and copy operational techniques from foreign groups. The fact that the pace of military deployments on all missions has increased is seen by many of these groups as “proof” of U.S. “imperialism”. These issues invite the targeting of U.S. military forces as the symbols and effective arms of these “imperial” policies or intended U.S. “hegemony”.

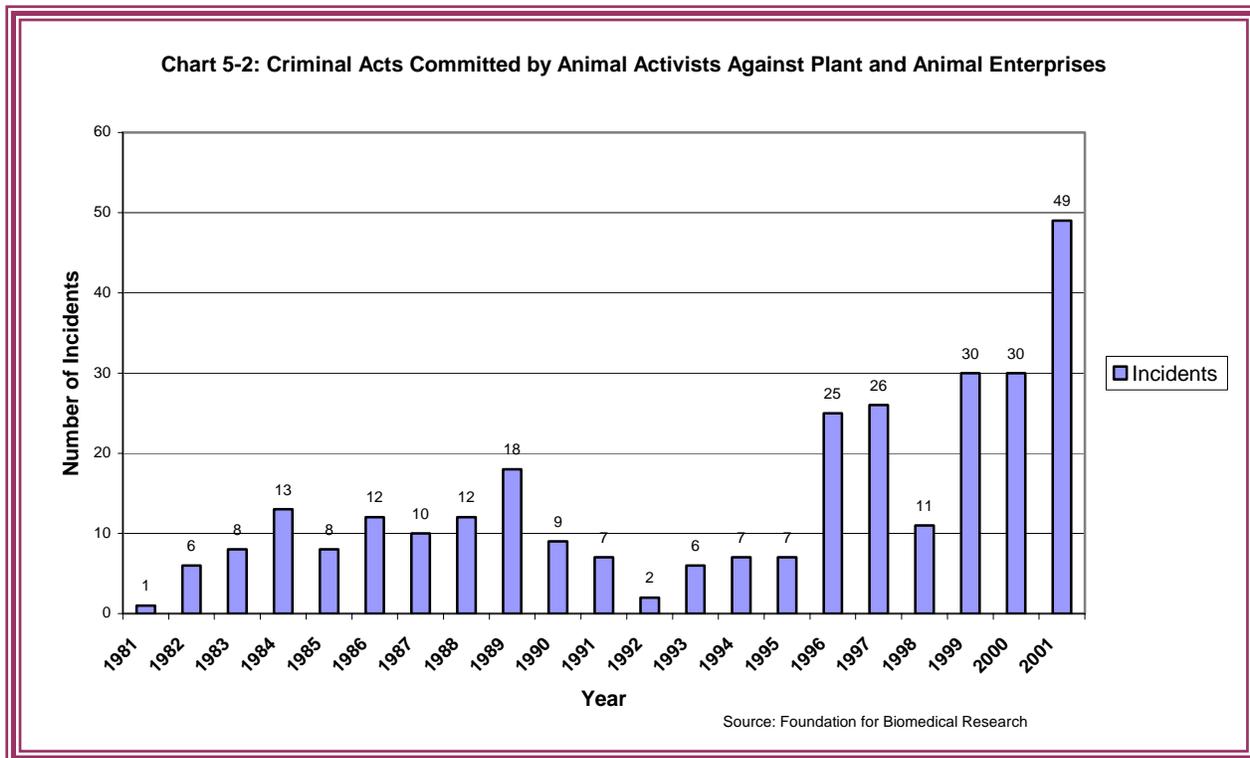
There is also the possibility of attacks directed against Army installations or personnel from single-issue terrorists focused on animal rights or environmental issues. The FBI considers these groups the largest domestic terror threat in the United States.¹¹⁴ Although these groups typically conduct arson, harassment, and vandalism, they have gradually increased their capabilities and rhetoric, threatening to “pick up the gun” and to target Federal offices and Federal and state law enforcement.¹¹⁵ It is expected that attacks are possible on range or post construction projects that they perceive as endangering animals, animal habitat, or the earth. Military research using animals for testing chemical or biological weapon antidotes or medical treatments could also spark direct action and harassment campaigns. Initially such attacks would be arson, vandalism and other forms of “monkey wrenching” – a term for sabotage combined with general mischief - but escalation is not only possible, it is likely. While claiming non-violence, letter-bombings and beatings have occurred in the course of these campaigns. Also, as observed in Chapter 2, when

¹¹³ Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999*, Report 0308, (Washington, D.C., n.d.), 27.

¹¹⁴ Congress, House, Resources Subcommittee on Forests and Forest Health, *The Threat of Eco-Terrorism*, Statement by the FBI's Domestic Terrorism Section Chief, James Jarboe, (Washington, D.C., 12 February 2002), 1; available from <http://www.fbi.gov/congress/congress02/jarboe021202.htm>; Internet; accessed 17 January 2003; and Robert Gehrke, “FBI: Earth Liberation Front Most Active Domestic Terror Group,” *Associated Press Newswires*, 12 February 2002, 1; available from http://www.stopecoviolence.org/pdfs/2_12_02.pdf; Internet; accessed 17 January 2003.

¹¹⁵ “From Push to Shove,” *Southern Poverty Law Center Intelligence Report*, no. 107 (Fall 2002), 4; available from <http://www.splcenter.org/intelligenceproject/ip-index.html>; Internet; accessed 17 January 2003.

terrorist organizations fail to achieve their goals completely and rapidly, an increase in violence and lethality inevitably occur.¹¹⁶ Chart 5-2 below shows the increase in criminal acts by animal activists since 1981. The data shows a 148% increase in incidents during the decade of the 1990s over the previous decade and the number of incidents just in the first 2 years of the 21st



Century nearly equaled the total in the 1980s.¹¹⁷

In looking at threats that involve facilities and infrastructure, we should also consider attacks on information systems and computer networks. Attacks directed against military systems, and designed to damage, not annoy, took place during the NATO air campaign against Serbia in 1999. Physical destruction of unprotected network components, or increasingly available technology that interrupts or damages computer circuitry from a distance may emerge as the most dangerous of these threats¹¹⁸, although malicious hacking and viruses will continue to be the most common.

Possible Threats

Although not as likely as attacks or thefts to obtain military equipment, direct attacks on installations by radicalized domestic groups are possible. Objectives for such attacks are based upon the groups' perception of the U.S. Government as illegitimate or oppressive. Most advocate a return to what they view as a sort of "golden age" earlier in U.S. history, or at least their

¹¹⁶ Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 177.

¹¹⁷ *Illegal Incidents Report* (Washington: Foundation for Biomedical Research, 2002), 1; available from: <http://www.fbresearch.org/animal-activism/eventssummary.xls>; Internet; accessed 4 December 2002.

¹¹⁸ Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999*, Report 0308, (Washington, D.C., n.d.), 40.

interpretation of it. This often centers around either increased states' rights or some strict, usually selective, interpretation of the U.S. Constitution. Traditionally "right-wing" groups have stepped up rhetoric and propaganda branding all government above county or state level as illegitimate. Ominously, much of the ideological material produced in this vein tends to dehumanize and advocate killing all nature of Federal Government servants, including and especially law enforcement and military personnel.

Lending credence to the possibility of these types of attacks, obvious symbols of Federal Government authority such as IRS facilities and Federal office buildings have been attacked repeatedly.¹¹⁹ Despite the inherent drawbacks to terrorist targeting of military forces discussed in Sections II and III, the chances of some sort of attack occurring are increasing. Attacks have been discovered in the planning and preparation stage (see the example below). Claims that control of the U.S. military has been usurped by hostile or conspiratorial foreign "forces"

Domestic Threat To U.S. Army Installations

From "Terrorism in the United States, 1999" FBI Publication #0308, Federal Bureau of Investigation

Between July 4 and July 11, 1997, the FBI, in conjunction with state and local law enforcement agencies in Texas, Colorado, Kansas, Indiana, and Wisconsin, executed multiple arrest and search warrants for a group of individuals planning an engagement with "foreign" troops stationed at the U.S. Army base at Fort Hood, Texas. The FBI was advised by undercover law enforcement officers that Bradley Glover, a self-proclaimed militia Brigadier General with a history of advocating the arrest of local law enforcement officers and members of the judiciary in Kansas, and an accomplice, named Michael Dorsett, anticipated an "engagement" with United Nations troops whom they believed were stationed at the military base. On July 4, 1997, after tracking the illicit activities of the two men, FBI Special Agents and officers from the Texas Department of Public Safety arrested Glover and Dorsett at Colorado Bend State Park, approximately 40 miles southwest of Fort Hood. Eight additional suspects were arrested and sentenced in Colorado, Kansas, Indiana, and Wisconsin for providing support to the operation.

encourages the targeting of military facilities and personnel.

As first discussed in Section III threats could also come from U.S. resident aliens or immigrant citizens with loyalties to ethnic, religious, or nationalist causes hostile to the U.S. or opposed to U.S. policies. As previously noted, these people may conduct operations as individuals or become operatives of existing groups. As "agents in place" – personnel already in the enemies' territory, and therefore less likely to be detected – they could be extremely dangerous and disruptive by merely working simple attacks as individuals or small cells. Modern information and telecommunications technology permits extensive linkages between immigrants and their home countries, and in some cases acts to preserve the individual's loyalty to the "homeland".

National Guard facilities and personnel are potential targets of attacks or sabotage to prevent counter-drug missions in support of local law enforcement. Since a significant amount of terrorist funding is obtained by drug manufacturing and smuggling, actions to prevent these missions or reduce their effectiveness could be in the terrorists' interests. However, these

¹¹⁹ Ibid., 52-61.

counter-drug missions would have to present a significant negative effect to the source of funds in order to provoke such attacks. Likewise, National Guard and Reserve members mobilized by their states or the Federal Government to increase security at high risk facilities in times of heightened alert may be targeted as a preemptive measure, or targeted as a statement by domestic groups against what they view as an encroaching “police state.”

Preventative Measures

Again, the heart of any program of preventative measures is denying the terrorist targeting information. Surveillance detection, OPSEC and counter intelligence activities all play a role in deterring and defeating terrorist operations. For the installation, the deployment of Military Police and other security elements are a flexible and responsive tool to react to increased threats. Coordination and liaison with local and Federal law enforcement is essential, as there will never be enough assets available to a post or activity to completely secure itself. Integration of existing guard posts, surveillance cameras, and other sensors into a network of coverage for the installation is a useful addition of capability to a protection plan. The comments in Section III on access control and the ease of document counterfeiting apply to installations and activities even more than to units.

The terrorist threat to non-deployable forces is a continuous one. It is not necessarily dependent on the imminence of conflict, but can be affected by U.S. foreign or domestic policies, and political currents that are uncontrollable or unknown to the military members affected. Installations and activities may be targeted for symbolic reasons, in pursuit of social or political aims, in order to delay or destroy deployment capabilities, to destroy support and logistics infrastructure, to drain military resources into increased security versus war fighting, and to steal military equipment and weaponry. The potential attackers range from transnational terrorist organizations and state directed terror groups to individuals of no formal organization. Given the complex and pervasive nature of this threat, and the immense value of non-deployable forces to the military, terrorism is a challenge of tremendous proportions.

Conclusion

This chapter examined the terrorist threat to military forces in three categories: deployed, deployable, and non-deployable. Although not all encompassing, it reviewed specific operations that terrorists may employ against military units in these categories and utilized historical examples to demonstrate the results. Preventative measures were discussed, emphasizing the importance of denying target information to the terrorist as a key to deterring and defeating terrorist operations.