A thread that has run through most of the preceding chapters is the possibility of prolonged threat campaigns. This appendix provides a detailed summary of our thinking on the matter of threat campaigns. As we see it, two types of enemy campaigns need to be considered:

- Those conducted independently of international events to punish the United States for imagined wrongs and injustices.
- Those carried out as a component of an adversary’s plan to prevent the United States from deploying its forces in response to a crisis in a distant theater.

**THE INDEPENDENT CAMPAIGN**

**The Threat**

In the case of independent campaigns, the threat could come from any number of quarters:

- One or two persons sharing a profound antigovernment animus (e.g., the Oklahoma City and Atlanta bombers).
- A small cell of amateur terrorists manipulated by professionals (e.g., World Trade Center bombing).
- Members of a transnational terrorist movement numbering in the thousands, with a salient religious imperative (e.g., Aum Shinrikyo in Japan, religious groups in Russia and elsewhere, bin Laden and al-Qaeda).
State-sponsored terrorists with superior capabilities and support. (Hoffman, 1999.)

**Campaign Objectives**

An independent campaign would seek to inflict pain, suffering, and damage—punishment for the “evil ways” of the United States.

**Illustrative Campaign Targets**

A punitive campaign may simply seek opportunities for mass killing and massive damage. Historical examples include the following:

- Using a biological agent or toxin, e.g., salmonella, to cripple an entire town (Rajneeshee group in The Dalles, Oregon, in 1984).
- Poisoning municipal water supplies (white supremacists in Chicago and Washington, D.C., in 1984).
- Blacking-out an entire state (Fuqra and Colorado).
- Toppling one skyscraper into another (World Trade Center).
- Simultaneous bombings in urban areas causing mass casualties (Bombay in 1993; Kenya and Tanzania in 1998) (Hoffman, 1999).

**Campaign Weapons**

In terms of the likely weaponry:

- Conventional bombs and arson remain the favorites.
- Specialty weapons, e.g., man-portable air defense missiles to attack troop transport aircraft could be used when available.
- State-sponsored or otherwise well-resourced actors (e.g., Aum Shinrikyo, bin Laden) may turn to WMD.

**Campaign Concept**

The operational concept for the independent campaign could be as follows:
• Avoid high-security targets and attack targets of opportunity.
• Make liberal use of hoaxes, risk real attacks less frequently.
• Take a leisurely pace since time pressure is probably minimal and results more from need to keep the conspirators motivated than from any requirement to accomplish specific levels of damage by a certain point in time.

A CAMPAIGN AS PART OF A BROADER CRISIS

Threat
The sources of threat probably are drawn from the same pool of actors as the independent campaigners, but state-sponsored actors and agents in the employ of the enemy (e.g., intelligence officers, professional saboteurs, special operations troops) are more likely suspects.

Campaign Objectives
Notional campaign objectives might include the following:

• Disrupting U.S. attempts to deploy its forces to the scene of a crisis overseas.
• Dissuading the United States from further involvement in the crisis by inflicting unacceptable levels of damage on U.S. territory.

Illustrative Campaign Targets
Campaign targets in this sort of campaign would tend to focus on military targets that could impede mobilization and deployment, and could include

• U.S. forces attempting to deploy from CONUS;
• departure airfields and ports of embarkation for U.S. forces;
• transport aircraft and ships;
• related power projection infrastructure; and
• to complicate the allocation of military forces, and to create widespread fear in the U.S. population, possibly attacks against “soft” civilian targets.

**Campaign Weapons**

The likely weapons include the following:

• Small arms, bombs, and arson, which probably will remain a mainstay.

• For state-sponsored and other well-resourced actors, such specialty weapons such as mortars, rocket-propelled grenades, and man-portable air defense missiles.

• For state-sponsored and other well-resourced agents, possibly WMD.

**Campaign Concept**

The campaign must give the impression that it is formidable both in breadth and depth and can continue its actions indefinitely, ultimately inflicting massive destruction on both military forces and civilian targets:

• The campaign requires prompt, effective attacks before U.S. forces can deploy significant numbers of units.

• Multiple (e.g., two to four) attacks will inflict severe damage on U.S. forces and prompt commanders to call a halt to the deployments until the security of the deploying forces can be ensured.¹

• Extensive use of hoaxes—particularly after an actual incident has established the credibility of the threat—will magnify the overall campaign’s effectiveness in waging psychological warfare.

---

¹This is consistent with the estimates in the Defense Science Board's 1997 Summer Study Task Force report.
THREATS AND RISKS

Because the bars to successful acquisition and employment are relatively high, one incident of a specific type (e.g., the use of WMD), increases the risk of other such uses.² Nevertheless, threats may aim at breadth rather than depth. In part, this is because targets of a given type can offer an attacker a finite number of approaches. Attacks in depth, therefore, run the risk of becoming stereotyped, leading to their perpetrators’ death or capture. Attacks in breadth, seeking different types of targets and different conditions under which the attacks take place, are likely to be greater challenges to U.S. security because they offer more and varied options for approach and attack. They also will convey the impression of a large, well-organized assault on the homeland and feed greater levels of concern. They will therefore be more attractive to would-be assailants.

Attacks in Breadth

Attacks in breadth may be widely distributed and involve a variety of targets. The enemy may attempt to exploit the “it can’t happen here” psychology by striking in very different parts of the country or striking only those targets that have not been hardened. As noted above, the targets themselves will probably be of different types.

Attacks in Depth

Attacks in depth are somewhat more likely to be part of a campaign supporting an ongoing foreign crisis. This is so because the enemy must accomplish specific objectives to disrupt the deployment of U.S. forces and dissuade the government from further involvement in the overseas issue. Therefore, the attackers must concentrate their efforts against U.S. forces and their supporting facilities. Even under these circumstances, however, the enemy may seek to limit his vulnerability by selecting different types of targets.

²In the language of Bayesian statistics, new evidence will force us to adjust the prior probability.
If this line of thinking is correct, the enemy might attack troops at ports and airfields, because a successful attack would not only kill deploying forces but might destroy important facilities, preventing them from being used again during the crisis.

**MEASURES OF PERFORMANCE**

To effectively counter an enemy campaign, the United States will need the ability to manage multiple, large-scale incidents. Fighting an enemy embarked on a campaign involves gathering intelligence about the campaign plan and taking actions to preempt and disrupt it, while also taking steps to defend against the attacks it plans.

To succeed in a countercampaign, the United States must have sufficient JTFs, RTFs, and other assets to respond to the individual attacks, but the country will also need intelligence and planning capabilities for the preemptive, disruptive, and protective measures that are also part of the countercampaign. Finally, recognizing that most JTFs are intended for specific missions and disbanded once those missions have been accomplished, the United States also may need a headquarters superior to the JTFs and RTFs that can command and control the overall effort.

**NOTIONAL PERFORMANCE LEVELS**

Notional performance levels for the performance measures described above include

- an ability to field two to four JTFs/RTFs over a prolonged campaign; and
- a headquarters capability for managing two to four separate JTFs/RTFs allocating resources amongst them, and synchronizing their activities.

**PROGRAM DESIGN ISSUES**

Two of the CONUS Armies, one on each coast, have dedicated RTFs, one called RTF-E and the other RTF-W. Because of the possible need for multiple responses, the other CONUS Armies should develop
plans for fielding additional RTFs based on the doctrinal and organizational developments in the two extant RTFs and based on whatever lessons are learned in exercises or actual employment.

While such key units as the TEU have multiple deployable assets, others, such as the USMC Chemical Biological Incident Response Force (CBIRF), are unique, and that could cause problems if multiple incidents occurred.

The responsiveness and capacity of the JTF/RTF and its components are also of concern, particularly in the context of a threat campaign that occurs during a mobilization and deployment, when mobility assets will be at a premium. Threat campaigns, we believe, could severely tax military response capabilities.