LANDPOWER ESSAY SERIES

No. 99-8 November 1999

Asymmetric Warfare and the Threat to the American Homeland

by

Joseph C. Cyrulik

America's unrivaled military superiority means that potential enemies . . . that choose to attack us will be more likely to resort to terror instead of conventional military assault. Moreover, easier access to sophisticated technology means that the destructive power available to terrorists is greater than ever. Adversaries may thus be tempted to use unconventional tools, such as weapons of mass destruction, to target our cities and disrupt the operations of our government.

Presidential Decision Directive 62, White House Press Release, 22 May 1998

Introduction

America has gotten used to the idea that wars occur elsewhere in the world, not here. When the American armed forces deploy to protect American lives and interests, it has always been "over there"—Iraq, Somalia, Bosnia, Kosovo and a dozen other places around the world in recent memory. Even Operations Just Cause in Panama (1989) and Uphold Democracy in Haiti (1994) were seen as taking place in remote countries, far away from America emotionally if not physically. War seems to no longer touch the American citizenry except "virtually," through the nightly news.

America's future enemies will not allow this comfortable naiveté to continue. The American homeland is just too inviting a target. Today the talk among defense planners, analysts and commentators is on "asymmetric" warfare—ways the weak can challenge and defeat the strong. This is nothing new. The military philosophy of ancient China's Sun Tzu, B. H. Liddell Hart's "indirect approach," Mao's and Giap's concepts of guerrilla warfare, and to a lesser degree even U.S. Central Command's "Hail Mary" single-pincer maneuver of the Gulf War, are all examples of asymmetric warfare—attacking your enemy where he is weak and avoiding where he is strong. That lesson is as old as warfare, despite the 1990s word-smithing update.

Landpower Essay Series is published by AUSA's Institute of Land Warfare. The series is designed to provide an outlet for original essays on topics that will stimulate professional discussion and further public understanding of the landpower aspects of national security. The content represents the personal opinions of the author and not necessarily the position of the Association of the United States Army or its members. Candidate essays of 5,000 words or less may be submitted to: AUSA Institute of Land Warfare ATTN: Landpower Essay Series, 2425 Wilson Boulevard, Arlington, VA 22201. For more information about AUSA and the Institute of Land Warfare, visit our Web site at www.ausa.org.

The United States military is immensely strong on the battlefield, perhaps even unbeatable with its superiority in information management, precision indirect fires and close combat. Only a fool would attempt to take on this juggernaut in a direct "symmetric" battle. A weak country that chose to challenge us would be forced to find another way. If the "rules" of warfare favor the stronger party, then the weaker party has motivation to change the rules, redefine the battlefields, and reframe where the war shall take place. This becomes a greater threat as our enemies and potential enemies are no longer exclusively nation-states. In the future our enemies may include such transnational actors as terrorist or substate political organizations, drug cartels and organized crime families, and even fringe-religious and cult groups. The rational opponent—and even the smart irrational opponent—will take the indirect approach, the asymmetric response to our conventional superiority. He will attack us where we are weak. Increasingly, that weak spot is our own homeland.

Already we are seeing a shift in the ways a future opponent might challenge us. China, a rising power with many interests contradictory to our own, is struggling with ways to take on the technologically superior United States. One suggestion from the Peoples' Liberation Army has been to focus on what they call "no-limit warfare." Proposed by two Chinese air force colonels, "No-Limit Warfare transcends all models of warfare, breaking with all limits, and using all means, particularly nonmilitary means, for an alternative alignment that is unique to us [the Chinese], striking at the enemy from all angles, at all levels and in all areas, to meet our war aims."[1] Simply put, this type of warfare focuses on a doctrine of asymmetric attack patterns against the homeland of a stronger opponent, using such tools as terrorism, information warfare and even weapons of mass destruction to undermine the opponents political will.

We are once again facing the frightening prospect of total war affecting the American homeland, because "The first rule of no-limit warfare is that there are no rules, with nothing forbidden, and all being transcendent."[2] In all conflicts since the War of 1812, our military has gone forth to fight the enemy military and impact upon the enemy's civil society, while *our* civil society remained largely invulnerable and unaffected. Now, with no-limit warfare, American civil society is once again a target. Correctly deducing that a less technologically advanced nation has no hope of catching up with or defeating the United States from a military-technological standpoint, an opponent will focus on new strategies instead. Such a concept will find favor with any nation that wishes to challenge the United States and avoid a direct technological confrontation.

Reasons for Attacking the Homeland

By attacking the American homeland (i.e., the fifty states and Washington DC, their people and infrastructure) an enemy gains a number of advantages. Besides bypassing our strength—the deployed combat forces in the field—the enemy is now free to target certain things that will help him defeat the United States and accomplish his political objectives.

First, he can attack the civil and military infrastructure upon which our military depends for power projection. As Sun Tzu said in *The Art of War*,

> To achieve victory without fighting is the acme of skill. Thus, what is of supreme importance in warfare is to attack your enemy's strategy.[3]

The American strategy is based on engagement and "shape, prepare and respond."[4] Power projection is the basis of that response. Since the end of the Cold War, most of our forces have been based within the United States. When we deploy for combat, peacekeeping or humanitarian operations, the troops, equipment and supplies often come directly from the continental United States (CONUS). Even for operations in areas where we have forces forward deployed, such as Europe and Korea, the split-based units would be heavily dependent on support and reinforcements from CONUS. To deploy, our forces in CONUS rely on the infrastructure used by the civilian sector.

An armored division is terribly hard to stop on the open plains of a battlefield; lashed to flatcars on a rail siding, waiting to be hoisted aboard a ship, it is harmless.

A campaign against the power-projection infrastructure in CONUS could be very attractive to an adversary. Central to much of today's military planning is the assumption that the American homeland will remain a secure sanctuary in all conflicts except strategic nuclear war with a peer.[5] While force protection, missile defenses and other measures are improved to guard our forces based or deployed overseas, bases in the United States are less well defended, and the civil infrastructure is virtually unprotected. Potential targets include seaports and airports where forces embark; railway infrastructure between bases and the ports; supply depots; barracks; high-value assets such as strategic bombers, Airborne Warning and Control (AWACS) or Joint Surveillance Target Attack Radar System (Joint STARS) aircraft; and the command, control, communications, computers, intelligence, surveillance and reconnaissance (C^4ISR) and battle management infrastructure (e.g., satellite communications and intelligence receiving stations, data transmission equipment, and even key personnel) needed to control the modern American military. The result of a campaign against our military infrastructure would be a delayed or crippled U.S. response to aggression overseas. For the enemy, the worst case would be to gain time to consolidate his gains and prepare for the American response. The best would be to make intervention too costly and time-consuming for the United States to undertake. In effect, such a strategy interdicts and begins to attrit American forces before they even arrive in theater.

While such a strategy offers a number of advantages to an enemy, attacking the power-projection base still takes on the American military directly. More important for securing long-term victory, an enemy can directly attack the will of the American people and their leaders instead, or in combination with military infrastructure attacks. It is a cliché that wars are fought for political ends and that the ultimate aim in war is to defeat your enemy's political will. Defeat the political will to fight, and you achieve victory without fighting even more completely than by attacking the enemy's strategy. In the United States, the political will of our nation and its leaders is the will of the people, and our people are vulnerable to a number of types of attack.

The aim of attacks against the American people would be to raise the level of pain felt by the United States for intervening. This pain can take the form of killing and wounding people, creating discomfort through attacks against the financial and transportation systems, and psychologically destroying faith in domestic institutions and systems. By killing and wounding people, damaging and destroying their homes and communities, disrupting their jobs and economic livelihoods and undermining their confidence and sense of security, an enemy can inflict pain to the point that the people demand a change in the government's policies. This is not to suggest that the American people are inherently weak or unwilling to accept pain or casualties—only that all people have a threshold of discomfort, danger or pain they are willing to endure for an objective, and that threshold is usually proportional to the importance of the objective. In Somalia, that threshold for Americans was seeing 18 of their soldiers, their fellow citizens, killed. In Operation Desert Storm, that threshold seems to have been far higher than what we had to endure. In the foreseeable future, with interventions into ethnic strife and complex humanitarian disasters, it is doubtful that America's survival or way of life will be threatened enough for the people to accept substantial pain to achieve victory. Certainly, when intervening in ethnic wars and conflicts spawned of ancient hatreds, the threshold of our enemies will be far higher than ours. Attacking the American people and their way of life, psychologically and physically, is a way of attacking our will. Defeat our will to fight, and the enemy most likely will achieve his political objectives.

Besides targeting political will and military infrastructure, a dedicated campaign against the American homeland weakens the health of the state and society as a whole for the long term. "Everyone in a society is affected directly or indirectly, and the bonds that unite a government, its

people, and its protective institutions are broken. Where such fragmentation exists, social cohesion is absent."[6] While it is almost impossible to think that American society is that fragile, a sustained campaign against the homeland could have long-term and potentially disastrous consequences for the American way of life.

Forms of Asymmetric Homeland Attack

The enemy has a wide variety of means from which to choose for threatening or attacking the American homeland. Some of these means are conventional or symmetric and represent the most expensive and least desirable options. Direct attack using air, land or sea forces would be virtually impossible, given America's size and location and her military dominance of the sea and sky. Ballistic missiles or cruise missiles launched from a submarine, surface ship or aircraft could be effective weapons but are expensive to develop, hard to conceal and difficult to deploy; they challenge our air and sea superiority directly, and invite retaliation, especially if weapons of mass destruction (WMD) are used. More attractive to a nonpeer enemy would be the various forms of asymmetric and covert attack. These could include, in ascending order of severity:

Psychological Operations/Propaganda Warfare/Media Warfare: Americans often think about being the users of psychological operations (PSYOPS) and propaganda to influence the will of another society. What is often overlooked is our own susceptibility to these methods. With our free press and media and increasing use of the Internet and computers for news dissemination, our society is increasingly vulnerable to sophisticated propaganda. Such operations could be as simple as setting up a Website to tell the "truth" to the American people (for example, the use of Websites by the Milosevic administration during the recent conflict in the Balkans), to much more elaborate operations that take advantage of new video and audio manipulation technologies and computer animation. In a few short years, it would not be impossible for an opponent to be able to "fake" a presidential address to the American people. Although Americans are more discerning about the information they get from the media due to our long experience with a relatively unregulated press, such an attack could sway a sizable proportion of our populace, or at least confuse the issue. An enemy could even commit an atrocity against his own people, frame the American military for it, and get it into the world mass media. Even if such an operation did not sway Americans, it could affect the perceptions of the world, to include our allies and coalition partners.

Narco-warfare/Crime: Just as terrorism has evolved to some degree into a state-sponsored activity, a weaker state could take advantage of the increasing sophistication of international criminal syndicates and drug cartels. By the same token, organized crime organizations have now reached such a level of organization and sophistication that they are able to influence the actions of nation-states.[7] Through either a nation-state's using a drug cartel or criminal syndicate, or a transnational actor's exerting influence on a nation-state, crime and drugs can now have a political-military effect. Flooding the American market with a particularly addictive or even lethal drug, or turning organized crime loose against our financial and business systems in the midst of an armed conflict, would help the enemy by weakening the United States.

Environmental Warfare/Terrorism: Closely associated with conventional terrorism aimed at killing people would be attacks against the environment itself. Americans are increasingly environmentally conscious, perhaps more so than any other people, and attacks specifically aimed at degrading the health of the environment would have serious psychological effects. These operations could include attacks on chemical plants, power stations and waste-disposal sites in order to cause massive and dangerous pollution: destroying oil pipelines; poisoning water supplies: sinking oil tankers off our coasts; or even spreading highly contagious diseases to crops or livestock as an adjunct to biological terrorism or warfare. While such attacks may not be decisive by themselves, they would further stretch the American response and damage our will.

Covert and Overt Sabotage/Commando Attacks: These attacks could be conducted by trained special operations soldiers or conventional terrorists and would be made against the above mentioned civil/military infrastructure needed to project combat forces. The persomel could infiltrate the country covertly and then change into uniforms before the attack (giving them prisoner-of-war status if captured), or remain covert to confuse efforts to retaliate. Additionally, covert terrorist attacks could be launched before the conflict starts and then be changed to "official" operations once hostilities begin, giving the opponent opportunity to degrade U.S. forces before they are committed. Operations could include scuttling a ship in the Savannah or Galveston channel to block sealift ships; destroying railroad switching stations, loading areas and equipment needed to transport Army units; destroying high-value aircraft at their home base with a variety of short-range stand-off weapons; damaging or destroying communications or intelligence facilities; and assassinating key political and military leaders. The United States would be forced to dedicate more forces to force protection while still in CONUS, and carefully timed deployment and sustainment operations would be delayed or disrupted.

Conventional Terrorism: What we think of as "traditional" terrorist acts, only more focussed and centrally controlled, could form the mainstay of attacks against the people and civil society. Carried out before the United States intervened as a way of "warning" America away, as well as after hostilities commenced to damage the political will, these sorts of attacks have the added benefit of being "deniable" by the enemy if he thought that beneficial. Terrorist cells would be established within the country long before an active conflict became likely. The FBI has already detected a significant and growing organizational presence in the United States by Hamas, Hizballah and other state-backed terrorist groups.[8] A key component of a terrorist campaign to support an enemy war effort would be to focus the attacks on politically influential sectors of the populace. By doing so, an enemy could break the political will faster than with an unfocussed terror campaign. Charles Dunlap suggested in his article "How We Lost the High-Tech War of 2007" that the elderly would be a key target due to their growing political influence and relative vulnerability.[9] Other demographic groups to be targeted might include parents (by attacking children in schools and day-care centers); middle-class families (by taking the war to suburbia and targeting movie theaters and malls); or even the entertainment elite and celebrities, by bombing or attacking studios and by selected assassination. These attacks would focus on making the people feel the pain of international intervention, influencing them to change the government's policies. Such attacks could also be aimed at dividing American society against itself by alienating some classes of society or causing fear and backlash against a selected ethnic group.

Information Warfare: One of the great asymmetric threats identified by American defense planners, information warfare (IW) would probably be a more effective tool for use against civil society than against the military. Military information systems are increasingly well protected against IW intrusion, but our civilian infrastructure is further behind. Information warfare attacks against financial systems, such as online banking networks and investment systems; transportation systems, such as municipal mass transit; the electrical power grids; and even entertainment outlets would cause discomfort and even pain in the American populace, acting directly against the political will. IW attacks would also act as force multipliers for sabotage, terrorism and propaganda operations, further disrupting American war plans and the lives of the American people. Several countries have or are developing robust information warfare capabilities, because developing this attack capability is relatively inexpensive, deniable and easily concealable due to the dual-use nature of the expertise and hardware.[10] While the actual effectiveness of pure information operations is still unknown, using it in concert with other operations could make it a powerful tool. For instance, taking down a city's 911 emergency system with IW while setting off terrorist bombs and interfering with the media could produce an *asymmetric synergy*, making the individual attacks much more effective than they would have been alone.

Covert WMD Use: The other great threat in the minds of defense planners—the use of nuclear/radiological, chemical or biological weapons against the American people or our military in CONUS—is the most serious asymmetrical threat. A nuclear device smuggled into a city, or a biological weapon released into the populace, could be the ultimate threat or the ultimate act. Used incorrectly, such an act could incite the rage of the American people to a level not seen since Pearl Harbor. Used at the right time and place, however, a WMD attack could destroy the people's faith in their government, in their military and in themselves. It could be a decisive attack against the political will of an entire populace. Even the threat of WMD use might have the potential to cause the American people to reevaluate their attitudes towards civil rights and personal liberty. A threat that causes Americans to live in fear, to trade liberty for security, and to change our way of life would make for a powerful tool.

Covert WMD use also has a degree of deniability. If an enemy launched a nuclear-tipped ballistic missile at the United States, retaliation would be swift and overwhelming. A weapon detonated within the United States through unknown means would limit retaliation if it could not be proved beyond a doubt that country X was responsible. Even if we were reasonably sure, it is doubtful that American and world public opinion would allow nuclear retaliation against a suspect. As the 1998 cruise-missile attacks against terrorist training camps in Afghanistan and a suspected chemical-weapons factory in Sudan proved, when you use military force for retaliation, you had better be sure of culpability. If an attack against the United States occurred and the guilty party remained unknown and unpunished, the faith of the American people in their government might be done incalculable harm. Besides the utility of WMD as terror weapons, such an attack could have a serious material effect on our warfighting ability, especially if used against a military base or staging area. The consequence management and clean-up after a WMD incident, as well as defense against further attacks, would use up resources needed for the fight overseas and further stretch U.S. forces. The chart below outlines some of the weapons available to an asymmetric foe.

Chemical Warfare Agents

Nerve Agents

- GA (Tabun)
- GB (Sarin)
- GD (Soman)
- GF
- VX (methylphosphonothioic acid)

Blister Agents

- HD – sulphur mustard (Yperite)
- HN – nitrogen mustard
- L – Lewisite
- CX – phosgene oximine

Choking Agents

- CG – phosgene
- DP – diphosgene
- Cl – chlorine
- PS – chloropicrin

Nuclear Warfare Devices

Fission Bomb
Fusion Bomb
Radiological Dispersal Device

Biological Warfare Agents

Anthrax
Botulinum Toxins
Brucellosis
Cholera
Clostridium Perfringens Toxins
Congo-Crimean Hemorrhagic Fever
Ebola Hemorrhagic Fever
Plague
Q Fever
Ricin
Rift Valley Fever
Saxitoxin
Smallpox
Staphylococcal Enterotoxin B
Trichothecene Mycotoxins
Tularemia
Venezuelan Equine Encephalitis

Source: Federation of American Scientists

Dealing with Tomorrow's Threats

Tomorrow's wars will be fought in two theaters with disparate means. One will be in our enemy's homeland, using the tools of modern conventional warfare; the other will be in ours, and the tools will be terrorism, sabotage and asymmetric warfare. A smart opponent will study us, our strengths and weaknesses, to devise how to fight and defeat us. He will look at our military, at our ability to defeat almost any other opponent, at our dominance of the sky and of the sea, and increasingly, of the realm of information, and he will see strength. Remembering the theories of Sun Tzu and Hart, and the lessons learned by the Iraqis and others, he will avoid our strength and attack our weakness. While we talk of the synergistic nature of remote fires, precision engagement, battlefield awareness and information dominance, he will see the synergistic nature of terror, deceit, brutality and unpredictability. Asymmetric synergy will be tomorrow's threat—the threat of multiple, simultaneous, diverse attacks against the will of the people and our national infrastructure in order to cripple or prevent our intervention in a crisis.

A war in 2010 might look very different from Operation Desert Storm or Operation Allied Force. As the political debate rages over whether America should become involved in some far-away conflict, terrorist cells begin to attack the fabric of American society. When America decides to intervene, these attacks grow to target our military bases. Planes are destroyed on the ground, trains carrying equipment are derailed, families of military personnel are attacked, and key communications nodes are destroyed. As the fighting in theater intensifies, so does the fighting in our own homeland. As precision-guided bombs rain down on the enemy capital, so low-tech bombs are detonated in ours. Financial and communications systems are crippled by unknown hackers or introduced viruses. Terrorist attacks prompt the rise of a dedicated and nontraditional antiwar movement. The synergy of many types of attacks occurring all over the nation nearly simultaneously from diffuse sources causes panic and undermines public support. Most serious of all, cities are threatened or attacked with biological, chemical or nuclear weapons, resulting in unprecedented casualties. America will no longer be a sanctuary in a turbulent world.

After more than 130 years of peace on American soil and after avoiding actual conflict on our own continent through two world wars and a global Cold War, warfare will once again return to our land. In the form of terrorism, sabotage, information warfare and propaganda, the enemies of the future will bring the conflict to us in order to defeat us.

The military and the govemment are now beginning to recognize the growing threat. The Defense Intelligence Agency (DIA) has said, "In general, we can anticipate an environment in which adversaries seek to avoid traditional conventional warfare with the United States, to pursue various strategies to preclude or diminish our military options, and to threaten or to use WMD."[11] DIA identified information warfare, infrastructure warfare and WMD terrorism as areas of particular concern. The American govermnent and military are beginning to respond. The Clinton administration's 1998 Presidential Decision Directives 62 and 63 on counterterrorism and critical infrastructure protection are steps in the right direction, as are the Department of Defense (DoD) initiatives on homeland defense.

To deal effectively with the asymmetric threat to the American homeland, the govemment and the armed forces must improve several key capabilities:

Interagency Command and Control Relationships: Defending the homeland and performing consequence management operations requires the capabilities of several departments and independent agencies, many with conflicting chains of command or little experience operating together. These include the Department of Defense (particularly the Army); the Department of Justice and the FBI; the Federal Emergency Management Agency (FEMA); the Transportation Department and Coast Guard; state and local governments, to include the National Guard; and many others. Figure 1 illustrates the organizational complexity of homeland defense.[12]

Changing Environment

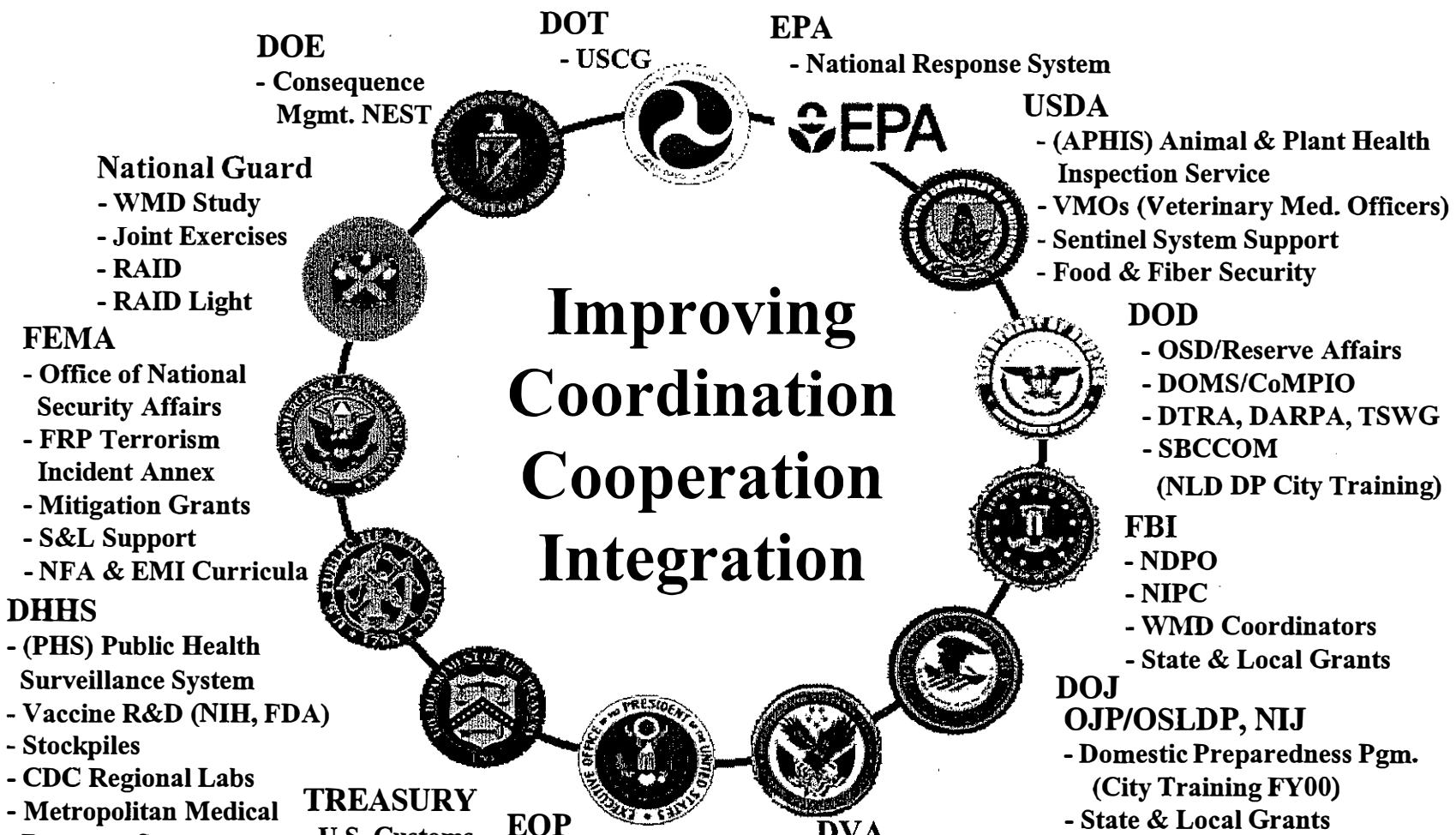

Figure 1

The efforts at coordination at the federal level, along with the increasing capabilities at the state and local levels, have provided the foundation for a new national framework for improving domestic preparedness.[13] Further legal and organizational issues must be resolved if all these disparate organizations are to work together effectively.

Intelligence Indications and Warning: Being warned is the first step to being prepared. The intelligence community must improve its capability to detect and warn of impending homeland attacks. This is an extremely difficult mission. The indicators of an attack have few if any signatures to be detected, and an effective campaign could be prosecuted by a relatively small cell. In recent years, the intelligence community has begun to organize to deal more effectively with potential asymmetric threats. The CIA's Crime and Narcotics Center (CNC), Counterterrorist Center (CTC) and Nonproliferation Center (NPC) all have responsibilities that involve them in defending the homeland from asymmetric attack.[14] These are difficult challenges that the intelligence community is now beginning to confront.

Consequence Management and Crisis Response: The FBI, DoD, FEMA, and state and local first responders need to be prepared, trained and equipped to quickly and effectively deal with the consequences of a major information warfare or covert WMD attack. Only effective recovery operations and certain retribution will help mitigate the physical and psychological impact of such an incident with the American people. Figure 2 defines the responsibilities of crisis management (with the FBI as lead agency) and consequence management (with FEMA as lead).[15]

Crisis management involves actions to anticipate, prevent and resolve homeland attacks, including identifying, locating, apprehending and prosecuting the perpetrators in a timely fashion. Consequence management involves protecting lives and property after an incident has taken place. The military, in the form of the National Guard's Rapid Assessment and Initial Detection (RAID) military support detachments, has a role to play in supporting both crisis and consequence management. The RAID teams, located throughout the country (see figure 3), are tasked to help local first responders identify the threat and coordinate further federal and state assistance.[16] While the RAID teams are an important first step, additional work is needed to extend RAID coverage, improve the capabilities of first responders, and establish extensive homeland defense capabilities with the National Guard and Reserve. The active-component military would have a critical role to play in support of any major mass-casualty incident within the American homeland, as they have the extensive resources and training needed to operate. However, that participation is conditional on a number of laws and regulations, including the Posse Comitatus Act, which forbids military participation in domestic law enforcement operations. The legal issues involved must be fully examined if the military is to make a significant contribution.

Critical Infrastructure Protection: This is another area where progress is being made, in the form of the President's Office on Critical Infrastructure Protection. Unfortunately, the threat could mature faster than the defenses. Also, while some critical information systems could be fully protected, the nature of modern information nets means that there is bound to be an overlooked weak spot somewhere. Military communications systems might be protected, but the civilian transmission lines that the military systems depend upon could be vulnerable. The rather amateurish information warfare attacks against U.S. and NATO Websites during Operation Allied Force in Kosovo only illustrate the potential for disruption from more advanced enemies.

Crisis and Consequence Management

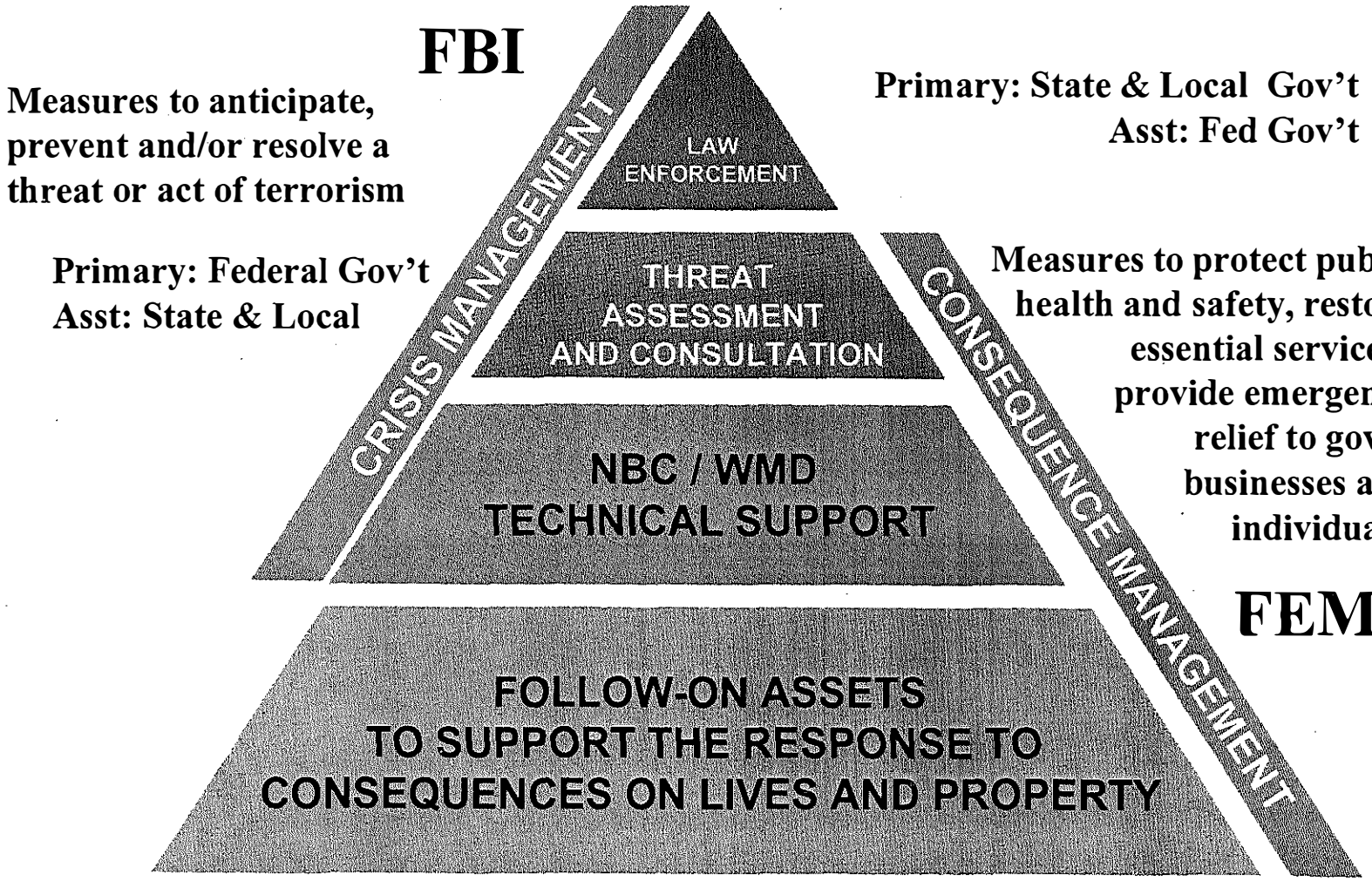

Figure 2

RAID Locations

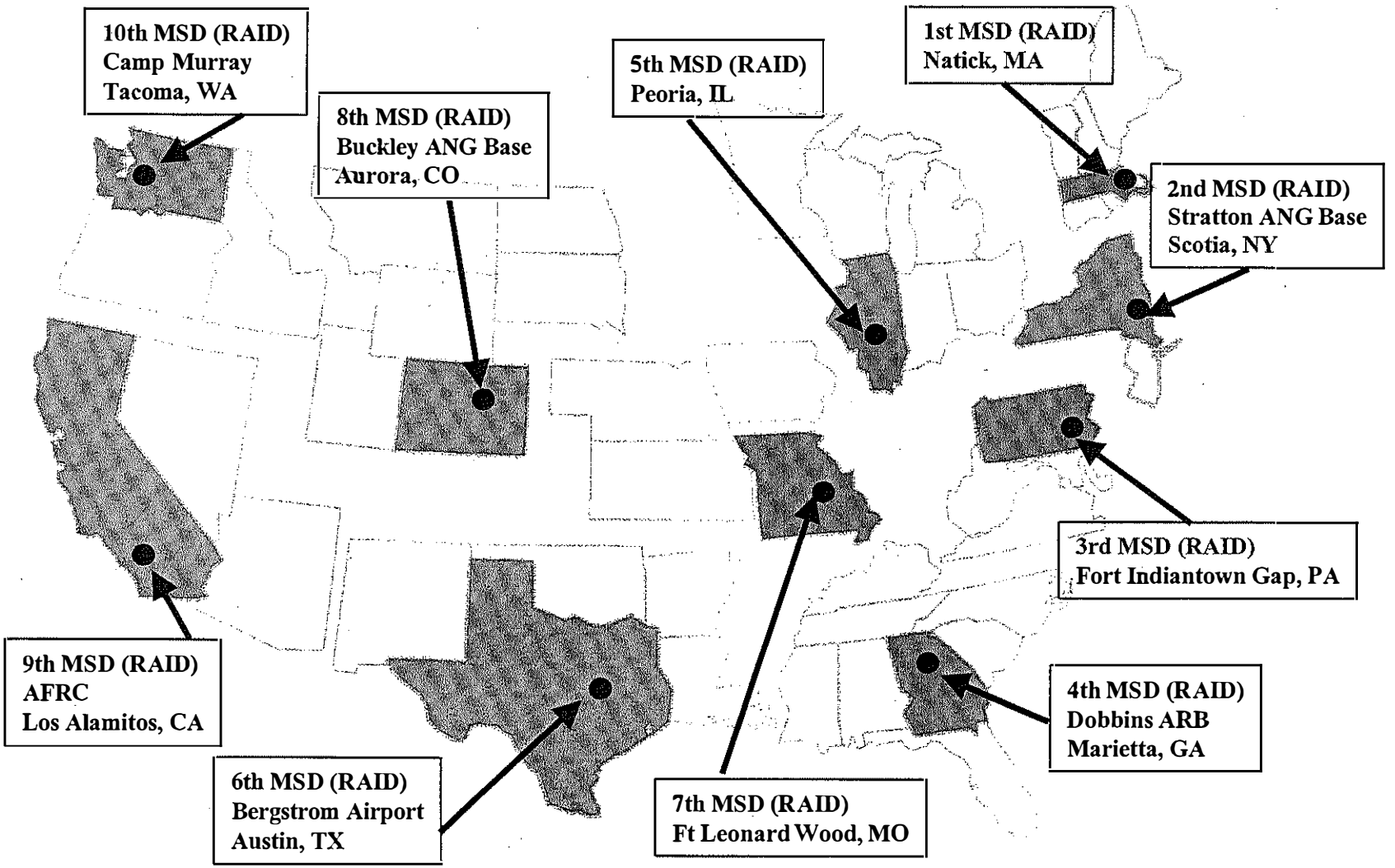

Figure 3

Conclusion

The rules of 21st century warfare will be far different from those of the 20th. Our enemies, incapable of winning using the rules we laid down, will change those rules. Defending against all possible threats is desirable, but we must focus our defenses on the most likely threat. An enemy would have to invest billions of dollars to even begin to match our superiority on a conventional battlefield, and we would still have a massive head start. An enemy desiring to challenge us will instead change the rules to suit his own advantages and to minimize ours. An enemy will attack where we are weak—our civil society. By preparing to defend the homeland now, before a clear threat emerges, we gain the initiative by forcing our potential enemies to start looking for a weak point all over again. We are the most powerful country in the world, and so we see little to gain by reexamining the rules of war. Our enemies and potential enemies can only gain by changing the rules. We must think as they will and anticipate their moves if we wish to retain our superiority.

Endnotes

1. Sha Lin, "Two Senior Colonels and No-Limit Warfare," *Beijing Zhongguo Qingnian Bao*, 28 June 1999, as translated by the Foreign Broadcast Information Service.
2. *Ibid.*
3. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1988). Note: This phrase has been quoted frequently and often appears slightly different depending on the translation.
4. Joint Chiefs of Staff, *National Military Strategy: Shape, Respond, Prepare Now-A Military Strategy for a New Era* (Washington, D.C.: Government Printing Office, 1997).
5. Fred C. Ikle, *Defending the U.S. Homeland: Strategic and Legal Issues for DoD and the Armed Services* (Washington, D.C.: Center for Strategic & International Studies, 1999).
6. Max G. Manwaring, "Security of the Western Hemisphere: International Terrorism and Organized Crime," *Strategic Forum*, Number 137 (Washington, D.C.: National Defense University, April 1998).
7. Major John Chenery, "Transnational Threats 101," *Military Intelligence Professional Bulletin.* July-September 1999, p. 5.
8. Dale Watson, Chief, International Terrorism, FBI, "Foreign Terrorists in America," Testimony before the Senate Judiciary Committee, 24 February 1998.
9. Charles J. Dunlap, "How We Lost the High-Tech War of 2007: A Warning from the Future," *The Weekly Standard*, 29 January 1996, pp. 22-28.
10. George Tenet, Director of Central Intelligence, Testimony before the Senate Armed Services Committee, 2 February 1999.
11. Lieutenant General Patrick M.Hughes, Director, DIA, "Global Threats and Challenges: The Decades Ahead," Testimony before the U.S. Congress. Reprinted by AUSA Institute of Land Warfare, March 1999.
12. Briefing by Major General Raymond F. Rees, Vice Director, National Guard Bureau, "The National Guard in Support of Local, State and Federal Authorities—Weapons of Mass Destruction," presentation to ILW Contemporary Military Forum, AUSA Annual Meeting, 11 October 1999.
13. *Ibid.*
14. George Tenet, *Director of Central Intelligence Annual Report for the United States Intelligence Community*, May 1999.
15. Rees, "The National Guard in Support of Local, State and Federal Authorities."
16. *Ibid.*

(Joseph C. Cyrulik is a Research Fellow with AUSA's Institute of Land Warfare.)