Between War and Peace: Deterrence and Leverage

by Frank Cilluffo and Robert Kupperman

Responding to the security needs of the United States at the edge of the twenty-first century reveals a myriad of new threats and challenges, many of which remain largely unappreciated by both policy makers and the public at large. As if the horrors of an impending nuclear war were not enough, we now face a new challenge to our national security--the indiscriminate use of weapons of mass destruction (WMDs) by terrorists.1 Because of the many complex policy considerations, the U.S. has yet to complete a strategic evaluation of this threat, which would identify actors, their capabilities and intentions, as well as preventative measures, crisis and consequence management, and response options. The overall framework for examining WMD terrorism continues to be viewed through the intellectual prism of Cold War strategic doctrine--mutually understood deterrence and rationality. Today's threat dynamics center around decidedly irrational actors--particularly rogue states and hostile non-state groups, who for reasons of ethnic, nationalist, tribal, economic, or religious hatred bear enmity toward the U.S. These patterns of hatred result in novel forms of conflict. Blended with the increasing availability of technology and knowledge relating to weapons of mass destruction and mass disruption,2 a grave new challenge to U.S. security has emerged.

Traditional U.S. preventative and response options are inadequate to meet the challenges of WMD terrorism. This article argues the necessity of modifying nuclear deterrence as a strategy for preventing terrorism involving WMDs. Having considered the dynamics of nuclear deterrence today, it is important: to understand the broadening nature of threats, both in terms of new actors (adversaries, and technology, weaponry and the manner in which it is employed) and their capabilities. The risk of a strategic nuclear exchange between Russia and the United States is low, but remains conceivable. Paradoxically, the likelihood of having to suffer a WMD incident is increasing ominous. Attacks by terrorists and other hostile non-state groups are not constrained by traditional means of deterrence. The threat of nuclear retaliation is difficult to mount against "actors without an address." As a result, U.S. policy must now be based on the assumption that nuclear deterrence could fail. Other prevention and response options must be identified to augment and complement traditional nuclear deterrence.

This article seeks to open new "policy space" and establish the essential principles of a new strategic doctrine, understanding and responding to the threat posed by WMD terrorism. Taken in isolation, WMD's are no longer the primary element in the zero-sum Cold War realpolitik. Because of the reduction in barriers to the acquisition and deployment of crude, but deadly, devices, WMD instruments are now available to both state and non-state actors. A fluid environment now exists in which the U.S. strategic deterrent is less effective in thwarting diffuse and irrational adversaries. A multitiered and multifaceted model of deterrence should be created so that the U.S. can identify and effectively apply leverage against the full range of threats. Such a policy would maintain a strategic deterrent to leverage other nuclear weapons states, but would also incorporate a broader spectrum of conventional military options and clandestine means, whether in support of law enforcement or covert action, as appropriate for deterring both rogue states and hostile non-state actors. Successful implementation and utilization of a multitiered and multifaceted strategy will require determining the appropriate deterrent for each threat. Intelligence collection plays a vital role in this determination, especially human intelligence (HUMINT) to determine exploitable vulnerabilities and to provid e timely intelligence indications and threat warnings--often inaccessible through any other method--to policy makers, before an incident occurs. Intelligence assets are also essential due to their flexibility in terms of rapid response and the ability to conduct clandestine operations.

The New Security Environment

Where We Were: Cold War Notions of Deterrence and Stability

The changing environment requires new preventative measures and responses. We have become witness to a change in the nature of conflict, regarding both targets and actors. The new battlefield incorporates the infrastructure of modern societies. Many critical nodes binding a technically based modern society are increasingly vulnerable to attack. The Cold War framework of indications and warning, diplomatic signaling, and escalation fire breaks that helped stabilize the U.S.-U.S.S.R. conflict is no longer

as predictive or useful. Such measures helped avoid nuclear confrontation and were the very paradigms that structured our forces and set forth the unwritten rules that governed the conduct of the actors during the Cold War. Further stability was added by the creation of the Single Integrated Operations plan (SIOP) and continuity of government considerations, which spelled out U.S. response options and plans for coping with a nuclear incident. Both sides afforded a greater measure of stability. Such ingredients incorporated into force structure, including offensive and defensive systems, were not the exclusive domain of the U.S. Civil defense and other initiatives aimed at protecting senior leadership and other critical assets were a cornerstone of Soviet defense policy throughout the Cold War. As should be expected, each side devoted its intelligence assets to understanding the capabilities and intentions of its principal adversary. A colorful but frightening assortment of trained maniacs armed with advanced weaponry is emerging. Such passive and active measures proved stabilizing and were nominally a part of each side's warfighting apparatus.

In examining today's challenges, it is necessary to revisit briefly the challenges of the Cold. In the strategic nuclear environment of the Cold War, the balance of terror was a game played by nations with mutually understood, but unacceptable, risks. It was a game of political leverage, amidst the cools of nuclear deterrence. In this contest between superpowers, armed confrontation risked leading to a catastrophic game of "chicken." As a result, direct confrontation was generally confined to the political and diplomatic arenas. Confrontations were intense and coercion undergirded the key strategies of deterrence. Nuclear leverage was a major facet of foreign policy. The threat of nuclear retaliation is less effective when weapons of mass destruction are no longer merely confined to "trusted" state rivals.

During the Cold War, both sides employed surrogates who used terrorism as a cognate of power; albeit the Soviets pursued this strategy much more aggressively. As a result, a colorful but frightening assortment of trained maniacs armed with advanced weaponry emerged, representing countries one day and their own personal interests the next. Actual military confrontation between the United States and the Soviet Union was largely indirect. This environment allowed the Soviets to exert its worldwide economic and geopolitical influence with near impunity. The challenge for American national security policy makers was to ensure that support for counter-insurgencies, interventions, and proxy wars initiated by the U.S.S.R. were contained sufficiently to guarantee that a catastrophic nuclear exchange was not an inadvertent result. This version of proxy warfare was a favorite of the former Soviet Union. It allowed the Soviets and their client states a cheap, highly leverageable form of warfare.3

For the United States, the primary policy objective was to prevent escalation by forestalling Soviet expansionism, limiting the possibility of a nuclear stand-off. With such a clear policy objective, it was possible to develop a vehicle of deterrence, which, among a rich assortment of deterrent tools, gave rise to the SIOP. Advertised as the central component of the U.S. strategic deterrent, the SIOP contained details of various U.S. retaliatory and first-strike options. Beyond the SIOP, the conditions in the aftermath of a Soviet nuclear strike were sufficiently clear to enable American policy makers to outline conditions for the continuity of government (COG). From this vantage point, U.S. policy makers were able to use analytical tools, such as war games and simulations, that further clarified the nature of possible nuclear confrontation. As a result, policy makers were able to identify the intentions and capabilities of the players.

Where We Are Now: Understanding Actors and Capabilities We can now ask if the emerging challenges are amenable to a clear understanding of the threat. A review of the capabilities and actors in the changing security environment reveals that similar delineations of response options and their consequences is largely precluded.

U.S. strategists must now counter the threats of mass destruction and disruption with a far cloudier picture of the capabilities and intentions of its adversaries. In light of these new imperatives, we argue that the U.S. Intelligence Community must undertake a fundamental review of its roles, missions, and priorities. Consequently, intelligence will play a critical role in creating a policy of direct action against both rogue regimes and hostile non-state groups who would employ the weapons of mass destruction against the U.S. or its vital interests. The security policy-making process is enormously complicated by fundamental changes in both the actors and capabilities confronting U.S. interests.

The Capabilities

The increased availability of advanced technology is strengthening the capabilities of hostile non-state actors. Their capabilities are further strengthened as the needed level of required knowledge and skill decreases while the power and technical sophistication of these technologies increases exponentially. Terrorist exploitation of these technologies makes them more difficult to counter because these actors arc increasingly utilizing sophisticated communications, plus counter-surveillance tactics and tradecraft. Without their demonstrated capability to cause chaos in society, many of these actors would remain at the margin, as they did during the Cold War. Instead, the proliferation of technology and knowledge about the means of mass destruction and disruption has empowered these actors, creating a new, modern class of adversaries--no longer operating at the margins, but upfront and center.

Quantum leaps in commercially available technologies have profound implications for society. We recognize that vast societal and business implications provide state and nonstate actors alike with an even greater body of capabilities than they presently enjoy. Already, the evidence of increased technological capability and availability to hostile groups is surfacing in the changing security environment; a striking example is the "loose nukes" dilemma in the former Soviet Union. The potential to wreak havoc and create unprecedented concern about nuclear, biological, and chemical terrorism is real.

Poor materials, protection, control, and accountability (MPC&A) safe-guards, procedures of nuclear materials and weapons storage facilities in the former Soviet Union, along with fears of a "brain-drain" of unpaid Russian nuclear scientists, have significantly increased the possibility of hostile state and non-state actors acquiring the capability to produce a nuclear explosive. Significant problems of corruption and poor morale within the military, security, and law enforcement communities in Russia facilitate the clandestine diversion of nuclear and radiological materials. The acquisition of such material by U.S. adversaries is dangerous not only because of the risk of use, but also because of transnational extortion. Terrorist groups could affect U.S. policy by threatening to detonate a nuclear explosive or even a radiological dispersing device within major urban centers. The MPC&A situation in the former Soviet Union raises the credibility of such threats to an unprecedented level.

While the United States has so far not been subjected to such an attack, we have not escaped the attempted use by terrorists employing weapons of mass destruction. In the February 1993 World Trade Center bombing, the perpetrators reportedly seeded their bomb with a cyanide compound. The threat apparently was neutralized because the killers did not know that the thermal shock generated in the explosion would be so great as to completely destroy the poison. But, if the terrorists had used radiological materials, such as Cesium 137 or Cobalt 60, there would have been no such salvation.

There are great technical barriers to being able to successfully monitor the movement of small quantities of nuclear materials globally, especially through the vast and porous borders of the former Soviet Union. Potentially weak MPC&A safeguards and procedures in China, Pakistan, and India may yield similar opportunities for diversion. Moreover, once successfully trafficked through any of these states into the hands of terrorists, no sophisticated delivery or dispersal system is necessary to employ a device.

While not without difficulty, the barriers to the acquisition and deployment of a crude radiological device are significantly lower than they were during the Cold War. Intellectual spillage of nuclear weapons knowledge and diversion of radiological material from the former Soviet Union could lead to a terrorist scrike.4 The reduction of Cold War era requirements for sophisticated delivery systems and large strategic doctrinal restrictions, like the SIOP, afford terrorists a significant advantage in time and flexibility. With fewer markers in the race to acquire and deploy WMDs, there are fewer stages at which government can reliably detect and interdict a terrorist conspiracy.

While no such strike has yet occurred, the consequences of even one nuclear incident in a major urban center, no matter how crude the device used, is unacceptable. Cold War era prevention and response options are of little value and the use of nuclear leverage, as was done during the Cold War, is no longer an option in such cases. The WMD threats of today include not only state, but also transnational nonstate actors, who have few political constraints.

Evidence of the difficulty to impose constraints on the use of WMDs by irrational rogue state and non-state hostile actors is well illustrated by the Aum Shinrikyo case. The sarin gas attack on the Tokyo subway line by this religious cult crossed a threshold, but there is no reason to assume that this is the only threshold of terror that remains to be traversed. Information warfare allows an adversary to electronically attack society's critical infrastructures. The use of sarin reflects the reality that WMDs are more available and can be produced and deployed in a matter of months. Sarin itself is easy to

synthesize. Any college laboratory with decent graduate students would permit the synthesis of sarin or any number of nerve agents. Aum Shinrikyo was also experimenting with biologicals, including pathogens such as anthrax, the continuous production of which is readily accomplished in a fermentation facility, similar to one making beer. Biologicals are not mere extensions of chemical agents or nuclear explosives. They are easy to produce and are frighteningly toxic. Because of the ease of acquiring pathogens, there is every reason to believe that the U.S. will encounter a terrorist incident involving biologieals.5

Not all of the capabilities involve mass destruction. Non-state actors are also capable of mass disruption. The principal methods and techniques in this arsenal are information warfare and infrastructure warfare. Information warfare allows an adversary to electronically attack society's critical infrastructures--telecommunications, electric grids, energy and power distribution, banking and finance, transportation, emergency services, and water and sewage supply systems--without ever stepping foot onto the target area or country. These infrastructures are also vulnerable to physical attacks, such as a well placed bomb at a critical node or key facility. An attack upon our financial systems or currency systems is a means of warfare the U.S. is unprepared to counter and defend against. Computer intrusion techniques deployed by Vladimir Levin to steal hundreds of thousands of dollars from Citibank, all from his terminal in St. Petersburg, are a harbinger of what is to come.

Information warfare is not confined to destruction, denial or disruption of service attacks, or theft and overt criminality. Deception and manipulation of information and images is a real threat due to advancements in mass media--psychological operations become weaponizable and can yield great leverage, directly targeting millions of observers, whether through television or the Internet. The most difficult aspect of the information warfare threat is that an attack can be launched from virtually anywhere by anyone. Furthermore, given the anonymity of 'cyberspace,' it is easy to conceal the true source of the perpetrator. As such, the source of the attack is unlikely to be determined. Compounding the challenge is that even if you do identify the true source of the attack, counter information warfare attacks may have marginal impact. This is especially true if the attacker is a terrorist or non-state actor with few electronic or infrastructure assets at risk.

The Actors

Today's stage cast of malevolent actors is driven by economic, nationalist, political, and the usual religious fervor. The real life saga which the U.S. and its allies are likely to encounter is far more difficult to codify into neat packages. Today we face familiar as well as new adversaries, such as Aum Shinrikyo, the mysterious nihilistic cult which, to nearly everyone's shock, burst onto the security agenda by dispersing an actual nerve agent in Tokyo's subway system, killing a few and injuring thousands. Only a poor dispersal device and a miscalculation of the subway's ventilation system prevented the death of thousands. The human tragedy, measured quantitatively in terms of numbers of deaths, is but a tiny aspect of the deeper psychological wounds that this pervasive cult attacked so cruelly. The militia movement, notorious in the wake of Timothy McVeigh's attack in Oklahoma City against his paranoid illusion of an obtrusive government, shows that little known actors can emerge from obscurity with one devastating act that brings their entire movement into the public spotlight.

There are a variety of motivations for terrorist activity in the changing security environment. Extreme religious, nationalistic, tribal, and ethnic hatred and conflict are on the rise. Such hatred is in many cases the fuel for deadly terrorist attacks. Whether it be a Ramzi Yousef planning to destroy twelve U.S. airliners in one day, an attack upon the world's financial cencer, or a radical fundamentalist Islamic faction in Saudi Arabia bombing a U.S. military barracks, there is substantial evidence to indicate that a considerable part of the ethnic, religious, tribal, and national hatred in the world is directed toward the United States and its interests. U.S. intervention in ethnic conflict also increases the risk of terrorist attacks. Rightly or wrongly, the U.S. is often perceived as intervening on behalf of one party in a multiparty dispute--angering the other party in the conflict.

The United States, to some, has long been viewed as "the infidel" or as "imperialist," whether it be the result of economic disparities, commercial jealousy, religious antipathy, or ideological conflict. Further, there is evidence to support the notion that the United States is becoming a target not merely for economic or political reasons, but increasingly for cultural differences as well. The revolution in global communications enables people in less developed societies--flocking to urban megaslums--to become increasingly aware of what they do not have. Direct Broadcast Satellite technology brings bewildering and

alluring images of American lifestyles from U.S. television into some of the most isolated areas of the world. The desire to acquire certain aspects of American popular culture or lifestyle can upset traditional cultural values in developing countries. American firms investing in new markets can encounter a minor backlash, such as the protest that greeted the opening of Kentucky Fried Chicken restaurants in India. More serious, however, is the threat of a backlash against U.S. popular culture assuming a more deadly posture--seeking to destroy or drive out U.S. investment by organized terrorist activity. As countries like Iran and China struggle to contain the spread of U.S. popular culture by banning satellite receiving technology and limiting Internet access, the risk of a radical backlash bears watching.

This brief snapshot of the diverse array of actors who threaten the United Stares should not exclude traditional state threats. Interstate hostilities remain critical, whether it be with "rogue" states or a return to conflict with resurgent Cold War rivals--Russia and, perhaps more likely, China. The end of the Cold War by no means represents an end of the nation-state, rather it is an era in which new international actors have emerged to challenge nation-states, at a level which was previously only attainable by other nation-states.

Dealing with Change: Strategies for Prevention and Response

In reviewing the threat of mass destruction and disruption, U.S. national security policy makers must consider the following questions:

How do we maintain stability in a world dominated by the proliferation of weapons of mass destruction and by intense sub-state conflict? While stability between states is increasing, stability within states is decreasing. The tensions formed between states in the bipolar period of the Cold War, when states were divided into Western and Eastern blocs, is no more. On the surface, the end of Cold War bipolarity is welcome because it reduces superpower interventionism and the risk that regional conflicts could escalate into nuclear confrontation. This gain for the international community, however, is offset by the increased instability within stares, and the emergence of intrastate ethnic, religious, and environmental conflict. This in turn, renders rational strategic deterrence ineffective and dramatically increases the possibility for WMD terrorism

The problems of WMD proliferation are critical because it reverses the escalation chain of the Cold War. Instead of a situation in which subregional and regional conflict could escalate to superpower intervention and possibly to a nuclear confrontation, we may now face a situation in which a crisis involving disaffected ethnic minorities reflects "instant escalation." As the amount of time and number of obstacles to acquiring WMDs diminish, the lure of a sensational and destructive attack could entice Chechen rebels in Russia or Islamic dissidents in Saudi Arabia to achieve their aims, or those of a rogue state sponsor, by striking directly at their adversaries using nuclear materials acquired from the black market or from rogue states themselves.

What are the implications and surge capabilities needed in terms of crisis and consequence management? A crisis involving WMDs in the United States would not be sufficiently thwarted by any form of SIOP strategy or COG program, because such plans have not been fully formulated for these types of contingencies, which are only now being addressed. Despite this, some key steps can be taken to ensure that both decision-makers and first responders (police, fire, emergency health) are prepared for terrorism involving WMDs or disruption. Such efforts should focus on education and training, particularly with respect to an improved understanding of the capabilities of terrorists.

Any response plan can only be based upon a complete understanding of the full scale destructive potential of a nuclear incident on a major urban center, or the massive potential for disruption contained in an attack on a major information network. For each type of attack, decisionmakers need to be informed with respect to the implications for continuity of government and continuity of society. In each case, analytical projections of civil unrest, impossible demands on medical services, heavy casualties and a severe political crisis should be considered. However, such a presentation of possible scenarios is for many too horrible to consider. Similarly, because the threat of mass destruction and disruption has to date remained largely theoretical, one cannot draw on historical analogies and the lessons learned. The Aum Shinrikyo attack provides a partial analogy, because despite their failure to fully disperse the Sarin, the attack still managed to throw the Tokyo firsttier responders into chaos. Still, no matter how difficult to contemplate, the effort to educate and train first-response personnel and political decision-makers must be made.

What type of deterrence strategies should be adopted? Determining the appropriate response becomes a key component of deterrence. As discussed below, intelligence will have to assume a key function. In addition to identifying threats, intelligence can also identify what is most valued by the enemy and what would make the enemy most vulnerable to deterrent measures. Responses include military reprisal, diplomacy, and economic sanctions, as well as the adroit use of law enforcement methods and covert action. The nature of the threatened response can be left deliberately ambiguous so that flexible retaliation is possible, enabling the U.S. to respond case by case, region by region.

The question of deterring an attack by means of mass destruction is highly contentious. Traditionally, deterrence has depended on states, but the discussion above illustrates that non-state actors acting on irrational and non-Western principles could be largely undeterrable. However, this does not mean chat deterrence should be abandoned completely. Conventional nuclear deterrence remains valuable as a means of discouraging state support of hostile non-state groups. The U.S. should signal that any nation whose political leadership can be implicated in either mass destruction or disruption attacks against the U.S. and its allies will be reciprocally targeted. This would include scenarios involving identification of active state intelligence officers, weapons or technology procurement, financial support, or training that knowingly contributed to the attack. Beyond this, the U.S. could signal to the leaders of non-state hostile groups that they will be held personally accountable for the actions of their subordinates and that the full weight of the U.S. military, as well as law enforcement and intelligence assets, will initiate a worldwide manhunt with the intent to reciprocate. These would be the new "rules" of U.S. strategy--we will find out what you value and we will show you that we can take it away if you attack us.

Intelligence Mission in Support of Prevention and Response Options

A multitiered and multitasked deterrent system is requisite to achieving an effective means of meeting threats from both hostile state and non-state actors. The success of the system would depend on a more robust intelligence capability for two fundamental reasons. Non-state actors acting on irrational and non-Western principles could be undeterrable. First, a robust intelligence base is needed in order to provide policy makers with the information they need to determine and maximize the best deterrence option on a case by case basis. Intelligence should determine which assets and vulnerabilities among U.S. adversaries can be leveraged to achieve deterrence. Clearly, a major state rival like China holds different interests than a non-state adversary like Aum Shinrikyo or Hezbollah. As a result, while valuable for state actors, the timeworn Cold War policy of "city for city" destruction is unlikely to be as effective for smaller non-state actors. The U.S. must identify vulnerabilities and show both state and non-state actors that they have a great deal to lose in any prospective action against the U.S. Intelligence will play a definitive role in determining how to counter non-state actors, whose interests and vulnerabilities are more difficult to identify.

Second, we need a more robust intelligence capability for gathering indications and warnings of imminent WMO threats to the U.S. and its interests abroad. Pre-incident intelligence is vital for deferring and disrupting WMD attacks. The central components of this strategy are identifying the intentions, motivations, and operational plans, and assessing the capabilities of U.S. adversaries. Insights into these areas should enable U.S. decision makers to identify the best tools for leveraging the adversary in a given situation. The tools include military reprisal, law enforcement, economic sanctions, official and back-channel diplomacy, and preemptive action and operations, such as clandestinely attacking the money supply and fund-raising initiatives of U.S. adversaries.

In the changing security environment where we face substantial threats from both state and non-state actors, U.S. intelligence assets must be more flexible and the Intelligence Community (IC) must be willing to reexamine collection methods. It is important that an efficient "mix" of intelligence collection methods be evaluated often, in order to keep pace with a moving target.

Accurate information on the motivations, intentions, and capabilities of non-state actors are more difficult to acquire. Viable solutions entail "all source" intelligence collection--however, greater emphasis must be placed on HUMINT. Largely through HUMINT do you obtain the first glimmers of information necessary to bring to bear the policy and physical weaponry of the U.S. Hostile non-state actors are diffuse, often highly compartmentalized, and increasingly aware of methods for avoiding electronic surveillance. In many cases, these groups are largely only vulnerable to compromise by HUMINT. HUMINT is less an analytical tool, than a tool of early warning. Technological intelligence (TECHINT) is a tool of precision,

but inflexible, in contrast with HUMINT. A recognition and utilization of these important capabilities by policy makers would be a major step in bolstering the U.S. HUMINT community, which has experienced uncertainty and declining morale.

Although successful for its original mission, the Cold War intelligence collection mix of HUMINT and TECHINT may be less effective for today's threats.7 Many failures can actually be attributed to the untimely dissemination of intelligence products and information, which are often poorly utilized by policy makers. Too often, inadequate "stove piping" has prevented the right intelligence--tailored to the consumer--from getting into the right hands at the right time. To use the economic analogue, a more consumer-driven intelligence cycle, in which intelligence users "pull" intelligence from the producers, rather than having consumers deluged by intelligence that is "pushed" is one means of improving dissemination. At a minimum, there is a need for a much clearer delineation of collection priorities. The best intelligence apparatus emphasizes the tailoring of intelligence, to ensure that tactical and readily utilized information is available to meet the different needs of the military and law enforcement.

For their part, policy makers and other intelligence consumers must recognize the inherent difficulties of HUMINT collection. Exploiting HUMINT sources creates a para.

This article originally appeared in the Winter/Spring 1997 edition of The Brown Journal of World Affairs *and is reprinted with permission.*