The Way to Missile Defense: Dealing with Russia and Ourselves

by R. James Woolsey

In its twilight months, the Clinton administration finds itself in a major dilemma. If it wants smooth relations with President Vladimir Putin’s Russia, it must leave the 1972 U.S.-Soviet ABM Treaty virtually untouched. But if it wants to mount an effective defense against North Korean, Iraqi, and Iranian weapons of mass destruction, and the ever-longer-range ballistic missiles these nations are developing, major revisions in the ABM treaty will be required.

Trying to Hit Small, Cold, Fast Bullets

The administration plans to begin its missile-defense deployment with 100 land-based interceptors in Alaska, guided by several land-based radars. Later, it may add another 100 interceptors at another site, and a few more radars. The GAO estimates that this will cost around $60 billion. To permit these ground deployments, the ABM Treaty would have to be amended in several important but relatively limited ways. As for sea-based systems, under a Protocol that the administration negotiated in 1997, but that has never been approved by the Senate, defenses on the Navy’s Aegis cruisers would not have the capability to intercept any Russian intercontinental ballistic missiles (ICBMs).

Now, in the face of the newly acknowledged threat from rogue states (or “states of concern”), the administration – because it believes it must minimize the need to amend the ABM Treaty – has chosen the more difficult and expensive of two basic ways to intercept attacking ballistic missiles.

Continued on page 2
The Way to Missile Defense ...  
Continued from page 1

Early in its trajectory, a ballistic missile is large, hot (because the rocket engine is still burning — i.e., in “boost phase”), and relatively slow. But when the boost phase ends and only the warhead is left, the remaining package is small, cold (hence hard for infra-red sensors to see), and fast — a much more difficult target. At this later stage, the target is traveling several miles a second. By this point, the customary analogy of “trying to hit a bullet with a bullet” is apt. This is what the administration’s system must do — flawlessly.

To make matters worse, even relatively primitive decoys or multiple warheads can, after boost phase, bedevil a defensive system. Other countermeasures, too, could be used to confuse defenses and hide nuclear or biological weapons among decoys. North Korea, Iran, and Iraq could develop or acquire this technology. The currently planned system also has purposely designed vulnerabilities in order to reassure the Russians. In late April, the Defense Department briefed Russian Foreign Minister Igor Ivanov on why the system’s radars would be inherently limited to handling only a few targets, and on our consequent inability to expand capability by adding interceptors.

Russia’s Temptations: China and Schadenfreude

There are two reasons why the Russians do not welcome our wasting $60 billion on the administration’s system: their budding romance with China, and a desire to see the U.S. fail at something — in a word, Schadenfreude. The Russians’ first motive was brought home to me this spring in a discussion with a senior general in the Russian ministry of defense. I tried out on him various possible approaches toward limited U.S. defensive deployments, but he continually returned to his first concern: China. It has become a tenet of Russian military thinking over the last few years that Russia must hold the world’s only superpower in check, and that a quasi-alliance with China gives them the best chance to do this. Consequently, any U.S. defensive deployment is an anathema to some in the Russian military if it might be effective, even if for only a few years, against a small Chinese ICBM force. The second point is that, for some embittered Russians, it is more important to deny something — security from ballistic-missile attack — to the lucky and prosperous Americans than to obtain it for themselves.

The ABM Treaty as Cold-War Antique

The time it was negotiated, many of us thought that the ABM Treaty was reasonable. The Soviets had a substantial advantage in large, land-based ICBMs, which may have proven able to destroy the U.S. Minuteman ICBM force. If the Europeans saw Soviet ballistic-missile defenses in addition to massive land forces and the threat to our ICBMs and bombers, they may have doubted our ability to conduct a retaliatory strike — giving us reason to doubt their steadfastness. All this might also have served to embolden Soviet leaders and cause them to make misjudgments. The ABM Treaty stopped the possible Soviet deployment of large-scale ballistic-missile defenses, thus protecting our ability to retaliate after a Soviet first strike. We traded something that Congress wasn’t about to approve anyway: a nationwide defense. Clearly, the world into which the ABM Treaty was born has vanished. The centerpiece of our nuclear deterrent is at sea, in the Trident submarines. We have no need to keep the Russians from deploying ballistic-missile defense; indeed, we might very well have reason to help them do so. Europe may feel decoupled from the U.S., but that has to do with genetically modified foods and banana tariffs, not Russian strategic superiority. There are no Russian land armies 100 miles from the Rhine; indeed, there aren’t really any effective Russian land armies anywhere at all.

It is objected that even though today’s circumstances are different, in the absence of an ABM Treaty the Russians will build more offensive missiles to penetrate any defenses that we build, and that this will foster a new arms race. But in reality, the Russian strategic problem today is poverty. The reason they want to move beyond START II, with warhead ceilings at 3,000–3,500, to START III, with ceilings of 2,000–2,500 (the Russians would prefer 1,500), is that they can’t afford to replace enough of their aging missiles and warheads to reach the START II levels. Their poverty has produced, especially among their military, a severe case of missile envy — they simply don’t want us to have more warheads than they do. They crave equality, on the cheap.

Continued on page 5
Book Review

Honey and Vinegar: Incentives, Sanctions, and Foreign Policy
Edited by Richard N. Haass and Meghan L. O'Sullivan
Brookings Institution Press (July 2000)
Pages: 168 Price: $16.95 (paperback)
Reviewed by Matthew Foley

Broad sections of the foreign policy establishment are reconsidering American policy regarding problem states. The term "rogue states" has fallen out of use in the State Department, replaced with the term "states of concern." The rationale behind this cosmetic change: states such as Iran and North Korea are more likely to change policies the United States considers objectionable if engaged in dialogue rather than isolated. Meanwhile, Congress has seen vivid debates about the merits of the sanctions on Cuba—the one of America's most enduring foreign policies.

Honey and Vinegar: Incentives, Sanctions, and Foreign Policy contains the intellectual vanguard for this reconsideration. Edited by Richard Haass and Meghan O'Sullivan of the Brookings Institution, the book argues that the punishing "stick" of sanctions can in some cases be made more effective by employing "carrots": rewards for positive behavior. Honey and Vinegar emerged from a Cantigny conference in the summer of 1999 underwritten by the McCormick Tribune Foundation and sponsored by the Brookings Institution.

A series of case studies drawn from papers presented at the conference provides the basis for a broad survey written by Haass and O'Sullivan. The editors summarize the lessons learned from previous policies regarding what kind of regimes are most receptive to engagement, and which policies are most likely to be effective. Each chapter presents a historical survey and then identifies how this attempt at engagement succeeded and failed.

The case studies repeatedly stress the need for domestic and international support for engagement policies. Lack of support can cause domestic political damage and weaken implementation. Johannes Reisner of the Research Institute for International Affairs in Germany found that internal criticism of the European Union policy of "critical engagement" toward Iran in the early 1990s helped bring the policy down. It was widely perceived as a thin rationale for lucrative investments in a regime that sponsored international terrorism. Additionally, the policy set the European Union against the United States.

Pauline Baker of the Fund for Peace writes that President Reagan's policy of engagement toward South Africa in the early 1980s suffered for the same reason. While the administration viewed South Africa as a long-time ally and bulwark against communism in its region, much of the public felt that the regime's domestic problems outweighed its diplomatic utility. Tracing the evolution of American policy toward South Africa and the response of the South African leadership, Baker argues that causing change in a country requires understanding the motivations of elites and of its constituencies. Foreign policy need not be so domestically divisive.

Paul Nitze School of Advanced International Studies Professor Frederick Z. Brown notes that changes in American domestic lobbying on policy toward Vietnam helped account for a change in policy over the past 25 years. Over time, business groups wanting to trade with Vietnam counterbalanced veterans groups that encouraged further sanctions.

James Goldgeier of George Washington University writes on U.S. - USSR relations in the 1970s as directed by Nixon and Kissinger. Goldgeier finds that the United States could not gather sufficient domestic support for detente. Nixon and Kissinger "oversold" the policy, initially promising too much in order to gain support. When the policy proved less than a panacea for relations with the USSR, domestic support waned. Kissinger's experience illustrates the need to have allies, Congress, and the foreign affairs bureaucracy on board for the implementation of policy. Neither the United States nor the USSR could ensure that all of its allies would accede to American and Soviet initiatives—both sides often expected the other to control its allies.

Robert Lee Suettinger of the Brookings Institution identifies three connotations of the term "engagement" in his chapter on U.S. - Chinese relations. In the broadest sense, engagement means contact on some level; the opposite of isolation. It can also mean the use of incentives and penalties to influence behavior. The third dimension of engagement indicates the importance of personal meetings among government officials, which can pave the way for continued commitment to good relations despite obstacles. As Suettinger describes engagement, part of its effectiveness lies in establishing personal contacts between leaders.
For this kind of trust-building to lead to tangible results, engagement policies should be well-defined. The vague and limited European critical engagement policy toward Iran helped doom the policy, according to Reissner. Brown describes the Carter-era American policy toward Vietnam as similarly vague, and consequently ineffective.

Leon Sigal of the Social Science Research Council emphasizes the need for mutual adherence to commitments. Unlike most scholars, Sigal argues that the United States failed to live up to its agreements in the 1990s with a generally predictable North Korea. He finds numerous instances of North Korean responsiveness to positive American and world signals, including the voluntary slowing of its nuclear arms program. When the North Koreans behaved as the United States wanted, they were neglected; for example, the United States fell behind its agreed schedule in its deliveries of oil and gas. North Korea understood that the best way to elicit a response from the United States was to threaten misdeeds.

Engagement policies are designed to change the incentives, and thus the behavior, of a regime. But if the engagement program is mishandled, it can create unintentional incentives and provoke behaviors opposite to its goals.

Kenneth Jaster, who served in the State Department during the Bush administration, writes that U.S. engagement with Iraq from 1988 to 1990 may have been the best of a variety of bad options. At the time, there was reason to believe that Saddam Hussein intended to adopt a moderate foreign policy. A key reason for the failure of engagement in this case was the lack of an American understanding of Saddam’s intentions. Jaster writes that the problems generated by this opacity reflect the need for sound intelligence.

Regarding China, Suettinger concludes that the United States has no other option but engagement. China is too underdeveloped to walk away from the United States, and too big to be intimidated by sanctions. Suettinger urges the United States to set clear goals, and understand the Chinese need for respect and reciprocity in negotiations. “Integration into the international community in the abstract is not an objective,” and is insufficient rationale for the Chinese to change their behavior. The United States should be prepared to use sanctions “sparingly and carefully” against China.

Some of the findings within the book’s case studies will draw fire—for example, Suettinger’s assertion that sanctions were not the driving force leading to Chinese cooperation with the United States on intellectual property. Sigal’s argument that North Korea has been a consistent negotiator. However, the argument for engagement is convincing. Many scholars and pundits in the early 1990s expected North Korea to implode under its irrational leadership. Instead, when backed into a corner, the North Koreans proved willing to moderate their behavior. Haass and O’Sullivan explicitly do not aim to make engagement the policy toward all countries; rather, they aim for it to be considered with equal weight when reviewing other potential policies, such as military action and sanctions.

The public’s attitude toward secretive engagement policies with states that violate human rights is uncertain. Haass and O’Sullivan make recommendations that will not be an easy sell to the American public. Political necessity may lead the United States to conceal the details of agreements. The editors argue that economically and strategically weakened countries with a centralized dictatorship are often the most receptive to engagement programs. Often, these regimes will have checkered records on human rights and foreign policy. Goldgeier writes of the problems of secrecy in negotiations encountered by Kissinger and Nixon: Baker writes of the strong domestic backlash against engagement with South Africa. Haass and O’Sullivan acknowledge these difficulties, writing that “engagement requires policymakers to expend at least as much energy in the U.S. domestic political realm as they do working with the target country.”

The editors have an excellent insight on the benefits of a failed engagement policy. In 1990, the United States was able to gain Arab support against Iraq partly because the United States had made every effort to treat Saddam’s government fairly. When an engagement policy fails, it sets the stage for greater international and domestic support for harsher actions. For example, Haass and O’Sullivan write that an American engagement policy toward Cuba would lend greater justification to the United States’ internationally unpopular policy, even if Castro remains unresponsive.

Future works, from Haass and O’Sullivan and others, will address the implications of engagement in greater detail. Haass and O’Sullivan present Honey and Vinegar as a case for the consideration of engagement policies, with recommendations for the kinds of policies likely to succeed. Their analysis in this book meets and surpasses those goals.

Matthew Foley is Communications Director with the National Strategy Forum.

Mark Your Calendar!
The Tenth Annual Review of the Field of National Security Law Conference will be held on December 1 and 2, 2000 at the Capital Hilton Hotel, Washington, DC. Watch for registration information in your mailbox or contact Holly McMahon at (202) 662-1035.
A Package Russia Shouldn't Refuse

Our principal concern is not really a bolt out of the blue fired by a North Korean or Iraqi madman, but nuclear blackmail. Much of the importance of ballistic-missile defense is that it can take away the tool that a Kim Jong Il or a Saddam Hussein could use to threaten us or our allies.

We therefore have to be certain that a rogue state would know that our defenses could be used in times of political tension. For this reason, localizing a deployment of boost-phase interceptors by putting them on land or aircraft near the rogue state is not a sound approach over the long run, since we can't be sure that we can maintain such deployments in all places where they might be needed. A Sea-based interceptor might be fine to deal with North Korea, but if you want to see an American naval officer collapse with laughter, talk to him about operating in the Caspian Sea.

One is thus driven to consider basing boost-phase defenses in space. Although the proposal of space-based lasers or other directed-energy weapons drew the derisory label "Star Wars," following President Reagan's famous March 1983 speech, there exists a considerably less exotic version of space-based boost-phase intercept: kinetic-energy interceptors. These would be very small satellites placed in low earth orbit and equipped with enough fuel that they could move into the path of a ballistic missile in boost phase as it rises, when the missile is big, hot, and slow. The collision would destroy the missile.

These small satellite-interceptors, termed "Burros" by one of their inventors, were designed to defeat most missiles of more than a few hundred miles in range as well as their countermeasures (but not, let it be noted, advanced Soviet missiles). A more ambitious version of this small satellite-interceptor program, termed "Brilliant Pebbles," designed to deal with advanced Soviet threats such as ICBMs with shortened boost phases, was receiving major emphasis by the end of the Bush administration.

The Clinton administration cancelled work on small satellite-interceptor programs, but there has been progress anyway. American communications companies such as Iridium and Teledesic have perfected the technology of launching many small satellites into precise low earth orbits with one launch vehicle over the last decade. If a Burro program were started, it could probably be deployed without the need to invent much technology.

A defense system such as Burros would have some major advantages in relations with our allies. Some allies see the currently planned land-based defense system as an expression of a Fortress America mentality, since it would protect us but no one else. Burros, on the other hand, could intercept in boost phase any ballistic missile of more than a few hundred miles in range, as long as the missile was launched within latitudes over which the small satellites were passing.

In addition, the fact that this type of space-based system can be localized—designed to cover only part of the globe—leaves open the possibility of an agreement with Russia. A Burro in an orbit designed to cover the northern tip of North Korea, for example, about 43 degrees north, would not pass over any part of the globe north of that line (nor any part south of 43 degrees south). Nor could it be diverted to perform interceptions substantially north of it. Virtually all of Russia lies north of 43 degrees north—including the areas where its ICBMs and submarines are deployed. All other countries against which we are likely to want to deploy defenses lie south of 43 degrees north, except for portions of China that extend north another ten degrees.

These facts raise some interesting possibilities. In a recent issue of Naval Institute Proceedings, veteran strategist Leon Sloss and his co-author Benson Adams, have proposed replacing the 1972 treaty with a new U.S.-Russian "ABM Reassurance Treaty" having essentially only one component: that the two countries agree not to deploy ballistic-missile defenses against each other.

The following package might be possible: We could propose to the Russians, under a new ABM Reassurance Treaty, that we would not deploy space-based kinetic interceptors north of some selected latitude. They would also agree not to deploy defenses against us. The limitations on Russia would perhaps have to do with radar locations and orientations, or with a similar limitation on satellite orbits.

As part of this package, we could offer some employment to the Russian military-industrial complex. For example, we could launch some of the satellites on Russian boosters. We could also offer to help Russia with its own defenses, e.g., against threats from the Middle East. It is very much in our interest that Russian early-warning systems operate reliably and don't mistake some other country's attack, much less the launch of an innocent Norwegian research rocket (as once temporarily occurred), as an American attack. Indeed, if Russian leaders wanted it as an interim measure before their own defenses were deployed, we could use Burros to protect Russia, since our system would cover launches from virtually any nation that might be a threat to it.

If Russia agreed to a new ABM Reassurance Treaty and subsequently turned totalitarian and hostile, we would still have the ability to withdraw from the treaty under the standard provision permitting withdrawal if an "extraordinary event" jeopardizes a nation's "supreme interest." We could then move to more effective boost-phase defenses, such as Brilliant Pebbles or directed-energy weapons, in order to be able to defend ourselves against Russia as well as rogue states.
As for Mr. Putin, he will need to decide where Russia’s interests lie. He cannot both help Chinese missiles obtain free passage across the Pacific and accommodate our need to protect ourselves from the likes of North Korea and Iraq. For our part, we owe China nothing on this point. We have no moral, political, or any other reason to make life easy for Chinese missileers. China is simply seeking a free ride across the Pacific for its ballistic missiles, on the back of an old U.S.-Soviet treaty. How do you say chutzpah in Mandarin?

If we deployed space-based defenses of any kind, China would, of course, threaten to build more ballistic missiles. But this would be a costly race for them, and one from which, in all probability, they would rapidly turn away – because we could add Burros much more cheaply than they could add missiles.

This point applies to rogue nations as well. Critics of ballistic-missile defense claim that if we defend ourselves, other countries will just be encouraged to build more offensive missiles to overwhelm the defenses. But if defenses are relatively cheap and highly effective, the incentives are reversed. By making ballistic missiles less valuable, effective defenses would discourage, not encourage, investment in offensive missiles.

Would Mr. Putin eventually buy this package? He would have to choose. Option A: unique treatment as a superpower in a new treaty-guaranteed relationship with us – one in which we do not defend against Russian missiles; investment from the West; being welcomed into the Western family of nations; and protection of Russia’s territory from ballistic-missile attack by other states. Option B: quasi-alliance with China; cool relations with us across the board; and the risk that the new U.S. president and Congress will refuse to accept any Clinton administration-Russian changes to the ABM Treaty, and simply go ahead and deploy what defenses they want against Russia as well as rogue states.

In defending our country, the next American president has plenty of cards to play, if he will but play them.


R. James Woolsey is former Director of Central Intelligence. He currently serves as Counselor to the ABA Standing Committee and as a partner in a Washington, D.C. law firm.

Catastrophic Terrorism...

Continued from page 1

Insurrection Act. or – even worse – simply to suspend due process under his supreme constitutional authority as Commander-in-Chief."

Dr. Hamre identified three impediments to problem solving in this area:

1. At a time when society is increasingly open, governmental legal authorities are based on physical borders.

2. There is an uneven distribution of authorities and resources in the federal system. Therefore, the need for realistic exercises to work through problems is imperative. For example, what are the effects on posses committatus and the chain of command if the National Guard is federalized?

3. There is a tension between peacetime efficiency and crisis preparedness. Budget cutbacks streamline government agencies for day-to-day activities, but reduce their ability to deal with large crises. The genuine need for efficiency is pushing government, like industry, toward “just in time everything.” There is a temptation to go first to DOD, but there are costs, including the paranoia of people who have watched Siege too many times and say the DOD wants to take over America.

Another example of the tension between “normal” and “crisis” governmental operations is due process versus the perceived needs in a crisis. Hamre remarked, “So much in government is about due process – taking the time, hearing people out, setting up mechanisms to arbitrate contending interests – exactly the sort of things you can’t afford and don’t have time for when you have a crisis. So there’s a profound tension between the nature of American democracy, with its deeply grounded procedural ethic embodying the principles of the Constitution, and what you really need in an extreme emergency situation.” Dr. Hamre offered three recommendations to improve governmental response to catastrophic terrorism:

1. Frequent exercises for high level decision makers.

2. Organizational change. What, for example, should be the role of the FEMA, DOJ, FBI, and DOD? Dr. Hamre prefers a low profile for DOD. As he pointed out, “Recommendations to get DOD into this become a lightning rod for the left and the right.”

3. An overall blueprint: “We have a tangled web, and everyone does it just a little bit differently.” Complicating the problem are the many “boutique” partial solutions offered, some of them politically driven. CSIS has a study underway on homeland defense to develop an overall picture of the problem.

Dr. Hamre closed with the thought that one of the strengths of democracy is that citizens themselves take an interest in understanding such problems and assist in their solution: “If you just say, ‘the government’s going to worry about this.’ it won’t get done. It’s going to come from the remarkable American institution of an intelligent and concerned citizenry that has a sense of civic responsibility.”
In a crisis situation, it is likely that the American people—and their representatives—would shift their priorities to some degree away from civil liberties toward increased protection. Ms. Spaulding noted, “Part of the responsibility of government officials, and those in this room, is to try to anticipate that and not necessarily take all the authority the American public would be willing to cede in that kind of situation, but to try to figure out what are the important steps that need to be taken and how can they be taken in a way that minimizes the infringement of civil liberties.”

Juliette Kayyem, of the John F. Kennedy School of Harvard University, emphasized that in the event of a catastrophic attack, “the normal rules will not apply.” Referring to the biological terrorism scenario, she discussed the legal issues from two perspectives: problems with the current legal regime, and how we should think about the law in a future catastrophic terrorism event.

First, a catastrophic terrorist event does not fit neatly into any perfect doctrine of law, either the rules of war, the rules of crime, or the rules of natural cataclysmic events. It may in fact fit into all three doctrines. Domestic preparedness for such an event must therefore include legal preparedness. She pointed out, “In many cases, the appropriate authorities may exist, but they may be hidden in a variety of doctrines of law.” Therefore, preparation should include stockpiling legal authorities and thinking carefully about the balance between effectiveness, civil liberties, and getting something passed. The danger of such stockpiling is that counter-terrorism legislation is an aggrandizing force and stockpiled authorities could become a new baseline rather than an exceptional case.

Second, many resources associated with catastrophic terrorism response are “dual use,” such as medicine, equipment, and so forth. In Dr. Kayyem’s view, counter-terrorism laws should instead be single-use (or, better still, never used), due to the potential for misuse.

Public Health Considerations

Barry Kellman of the DePaul University College of Law observed that “Law is the antidote to panic. If officials respond effectively and judiciously to a catastrophic terrorism event, then the event will demonstrate that our system of government and rule of law offer a richness and vitality capable of sustaining our way of life, even in the face of a great tragedy. To the extent that that capability is apparent in advance, it serves to diminish the terrorist incentive to commit the attack in the first place.”

Physicist Lisa Gordon-Hagerty, Director, Transnational Threats, National Security Council, highlighted the importance of the local “first responders” to a domestic terrorist incident. The federal role would begin from two to eight hours after the attack, with the knowledge that no two metropolitan areas in the country are the same. The question is how best to use the equipment and resources available. Further complicating the equation is that the responses to chemical, biological, and radiological or nuclear incident are quite different. She emphasized that the federal government is aware of the increased risk from biological agents and is focusing its attention on that threat. The problem is magnified by the residue of the frightening biological programs of the former Soviet Union.

Dr. Tara O’Toole, M.D., of the Johns Hopkins Center for Civilian Biodefense Studies made three points about the response system to biological terrorism. First, the health care system has very little surge capacity to deal with a catastrophic attack. The biggest problem is staffing, although equipment is a problem, as well: even in normal times the Johns Hopkins Hospital must rent a dozen or more ventilators to meet the demand. One study determined that Baltimore—with two medical schools and 13 hospitals—could not handle a situation requiring 100 extra ventilators. Interesting legal issues also arise. May hospitals close their doors if they are overwhelmed? What if they deliver substandard care? What if medical and ancillary personnel refuse to work in a highly infectious environment? Second, there is a problem of situational awareness. Is an outbreak of disease due to an attack? If so, how extensive is the attack? The public health system tasked with answering such questions has been underfunded for decades and does not interact well with the health care system. Third, the 21st Century will be the age of “big biology,” just as the 20th Century was an age of “big physics.” “Every advance in biotechnology and genomics will create the potential for more potent and more diverse bioweapons. The more we know about antibiotic resistance, the better able we will be to engineer it into organisms.”

Gene Matthews, Legal Advisor to the Center for Disease Control, focused on the status of public health laws applying to bioterrorism. The chemical terrorism situation is well handled by the emergency preparedness laws. State laws must address three categories of events: access to records, control of property, and management of persons. Many of the laws on the books were written some 80 years ago and have not been used for the last 50 years or so. There are not many with a memory of how to apply these police powers. Additionally, it is not clear how they would withstand the sort of judicial scrutiny applied since the Warren Court in matters of individual rights and due process. Health authorities need to understand that they are not a service delivery organization, but a police power. He pointed out that “a lot of us in the public health legal community have known for years how antiquated the laws are.”

Discussion highlighted the importance of effective communications in a crisis. One technique is to ensure that figures of moral authority in the various communities in an area understand the issues and can explain them. Quarantines pose particularly thorny problems and are very difficult to enforce.
The Role of the Military

Michael Wermuth, Senior Policy Analyst at the RAND Corporation, raised the question of posse comitatus: the legal restrictions on using regular military forces in a law-enforcement role. He pointed out, “there are numerous statutory exceptions to posse comitatus and the actual use of the military as a result of that. Most notably, the insurrection statutes, 10 USC 331. et seq., to integrate the schools in the South and to respond to major riots in U.S. cities.”

Rear Admiral Michael Lohr, Deputy Judge Advocate General of the U.S. Navy, said that DOD views itself in a supporting role, rather than as the lead federal agency. With respect to crisis response, the military has a number of helpful capabilities. These range from technical advice to the employment of military force. The former is permitted under Chapter 18 of Title 10, U.S. Code, and the latter is greatly restricted by posse comitatus: “a useful firebreak for not over-relying on the Department of Defense.” The posse comitatus rule applies unless “action is necessary for the immediate protection of human life, and civilian law enforcement is not capable of responding and dealing with that threat.” This is a necessarily difficult test. The Defense Department can also be helpful in consequence management. DOD has a history of providing disaster relief assistance through FEMA, under the Stafford Act. Other authorities could also be invoked, including the insurrection statutes. Admiral Lohr noted in conclusion that the “rules of engagement” terminology has been discontinued in the context of domestic support operations in favor of the FBI’s “use of force” rules. He pointed out, “We’re trying to train 18 and 19-year-old kids who we want to be warriors to be cops on the beat.”

Judith Miller, former General Counsel, Department of Defense, said that the enormous capabilities of DOD virtually ensure they will be called up to assume a major role in a terrorist response. As noted earlier, DOD is much more comfortable providing support than being in the lead. A great deal of public good will could be lost if DOD is perceived as just another police force, and in any case the training is so different that switching in and out of the police role is difficult. She noted, “Interactions with the American public in a law enforcement capacity, will end up risking some of the confidence and respect that they deserve in their regular roles, because they haven’t been trained effectively to deal with the American public in a law enforcement role.”

Stephen M. Duncan, former Assistant Secretary of Defense, emphasized that DOD is not sufficiently prepared for this mission. Quoting a CSIS study, he said, “inadequate or insufficiently understood legal authorities for a military role in homeland defense against a broad base of WMD [weapons of mass destruction] is also a major national security concern.” In the event of a major attack, use of military forces in law enforcement will be more widely accepted. Suzanne Spaulding cautioned that DOD might well play a leading role under certain circumstances – even helping to enforce a quarantine – and should plan for what they are going to do.

But there is a danger in military law enforcement efforts, as pointed out by Elizabeth Rindskopf Parker, Chair of the ABA Standing Committee: the likelihood that “accidents and worse will inevitably happen” due to the complex training required to do law enforcement and the degree to which the “rules of engagement” mentality necessarily dominates in the military.

Law Enforcement Authorities

Robert M. Blitzer, Associate Director for Counter-terrorism Technology and Analysis at SAIC and former Domestic Terrorism Section Chief at the FBI, said that the necessary legal authorities for counter-terrorism law enforcement are on the books: There is sufficient authority even to collect intelligence inside the United States, although there is necessarily a higher standard when dealing with U.S. persons. One problem, however, is the need to open a preliminary investigation focusing on just one person. A separate set of domestic terrorism guidelines for the FBI field agents would be helpful.

With respect to the dissemination of information, there are 26 joint terrorism task forces located around the country, with state, local, and other federal agencies working with the Bureau. The system has worked well, and the Bureau has been able to share information without compromising sources and methods.

Portsmouth, New Hampshire City Attorney Robert Sullivan shared his perceptions from a local level about the May 2000 “Top-Off” exercise, which simulated a chemical attack on his city and a biological attack in Denver, Colorado. He emphasized the role of local “first responders,” who necessarily will be first on the scene and may well be the best ones to handle the situation as time goes on. The tendency of federal law enforcement to step in and try to take over was not helpful, and they disregarded a fully functional emergency operations center set up by the city of Portsmouth. He remarked, “The nature of every single one of these guys was they wanted the control. ‘It’s my site; it is my site.’ This is Portsmouth. my site.” ‘This is a federal thing, it’s a bomb, it’s ours.’ And they fought. They stood in a circle and fought with each other over these things, while bodies rolled in the field behind them. It was not a pretty picture.” In any case, new criminal laws are not needed: “Every event that happened at Portsmouth, in addition to being a terrorist act, was also a violation of state law.”

Gene Matthews noted in the discussion that public health laws might need to be reviewed to ensure they meet current procedural guidelines.
Michelle Van Cleave, President, National Security Concepts, concurred with the view that the laws are sufficient, but “authority is not the same thing as ability” and practice and training are necessary. How authorities would be interpreted in practice is crucial, and it may be time to consider updating them.

Kate Martin, Director, Center for National Security Studies, warned that certain changes under the Foreign Intelligence Surveillance Act have made the system less transparent, and it is harder to convince outsiders that authorities are being exercised in a constitutional manner. Secrecy erodes the trust and confidence of various U.S. ethnic and racial communities.

**Intelligence Authorities**

Elizabeth Rindskopf Parker noted the role of intelligence is “to preempt, to anticipate, to prevent the problems of coordination that we have so graphically discussed.” How can we then preempt such actions so that such problems of coordination do not arise?

Stewart Baker, former General Counsel for the National Security Agency (NSA), began with the issue of cyber-terrorism, which he believes for the foreseeable future “is a weapon of mass annoyance, not a weapon of mass destruction. If your email went out for a week, you’d take a vacation.” There are limitations on contacts between the FBI and the White House. For example, the Justice Department will not permit a White House briefing by the FBI on a criminal investigation unless the Deputy Attorney General reviews the contents of the briefing in advance. “It’s hard to imagine that working well in a crisis.”

There is sufficient authority to collect intelligence against foreign nationals, but Executive Orders, in particular, limit what NSA does against U.S. persons. In a major crisis, these restrictions are likely to be lowered. One problem is the anonymity of the Internet, as “anonymity is not generally consistent with ordered liberty.”

Richard Shiffrin, Deputy General Counsel for Intelligence, Department of Defense, emphasized the “extraordinary capabilities” of the intelligence community: “With respect to anticipation and indications and warnings, we do it all the time. 24 hours a day, seven days a week, and have actually been effective in interdicting a number of possible incidents over the past few years.” There are, however, some limitations:

1. The nature of the threat is changing. The Soviet danger has been replaced by a transnational and possibly not state-sponsored threat.
2. Technological changes such as fiber-optic communications and strong encryption complicate intelligence gathering.
3. Finite resources require the setting of priorities, but we only have so much money, personnel, and time. We collect a lot of information, but we don’t collect or analyze all of it. So we have to figure out where we want counterterrorism in our overall setting of national priorities for intelligence.
4. There are necessarily policy limitations due to the very intrusive nature of intelligence operations.
5. There are legal restraints, although they are not unwarranted and they do not “in any way stymie our ability to do an effective job.”

It is important to maintain a balance in intelligence operations, Mr. Shiffrin concluded. If NSA collects and disseminates too much information, even in the counterterrorism field, people might conclude, “We don’t like NSA listening to everything all the time,” which would likely prove fatal for NSA.

Eugene Bowman, Associate General Counsel, FBI, noted the dramatic increase in the terrorist threat in the United States, especially over the last two years. To do its job effectively, the Bureau needs continued public support, and the Attorney General’s guidelines set useful limits on how things are done – particularly in view of the increasing threat and necessarily more intrusive nature of FBI activities. He observed that intelligence information is now coming to law enforcement for criminal as well as intelligence purposes, forcing a re-evaluation of how it is to be used. In addition, technological change is so rapid that new equipment has a shelf life of about 90 days and it is often necessary to gain physical access to a computer to decrypt messages.

Dr. Williams is on the faculty of the Department of Political Science, Loyola University Chicago. His most recent work (with Charles C. Moskos and David R. Segal) is “The Postmodern Military: Armed Forces After the Cold War” (Oxford University Press, 2000). He may be contacted at jwillia@luc.edu. The McCormick Tribune Foundation will publish a full conference report in the fall.

**Call for Nominations!**

The Committee is currently seeking nominations for the Morris I. Leibman Award in Law and National Security. The Award recognizes the example of Mr. Leibman’s lifelong dedication to the rule of law, leadership in the field of law and national security affairs and continuing support for those engaged in this field. Nominations must be received by October 16, 2000. If you have not yet received a nomination package or for additional information, call the Committee offices at (202) 662-1035.
Trolling for Terrorists:
New Report Outlines
Surveillance Authorities

by William C. Banks

The counterintelligence business is booming, at least in relative terms. Attorney General Janet Reno reported to Congress this April that in 1999 the Foreign Intelligence Surveillance Court (FISC), a secret court created by Congress, approved 886 secret warrants, more than in any previous year, and that as in all prior years, no applications for surveillance were modified or denied by the FISC.¹

In at least one case, however, congressional investigators and an internal Justice Department investigation concluded that the FBI and counter-intelligence officials were needlessly restrictive in interpreting statutory constraints on intelligence collection. In deciding whether to pursue electronic surveillance of Wen Ho Lee, the Los Alamos scientist suspected of spying for China when he copied secret nuclear weapons files to his home computer, Justice Department lawyers said they could not satisfy even the relaxed statutory standards for national security surveillance,² much less the traditional law enforcement requirements.³ Indeed, the President’s Foreign Intelligence Advisory Board concluded last June that investigators focused their espionage investigation on Lee without hard evidence that classified warhead data obtained by the Chinese came from Lee or anyone else at Los Alamos. But the Justice Department report concluded that counter-intelligence officials simply did not seek the surveillance that they were entitled to conduct.⁴ This surveillance dispute reflects the ongoing turf battle inside the Justice Department between those seeking intelligence information and those responsible for enforcing the criminal laws.

By contrast, a report from the European Parliament on Echelon, a worldwide surveillance network used by the National Security Agency and several U.S. allies to intercept overseas telephone calls, faxes, and email,⁵ prompted concern that legal authorities to conduct electronic surveillance might be abused, at the expense of personal privacy. Reacting to the Echelon study, in the fiscal 2000 Intelligence Authorization Act, Congress called on the Director of Central Intelligence, the Director of the National Security Agency, and the Attorney General to prepare a detailed analysis of the “legal standards employed by elements of the intelligence community in conducting signals intelligence activities, including electronic surveillance.”⁶

This February, the required report was submitted.⁷ Although the report contains a succinct and straightforward description of the legal authorities for conducting electronic surveillance, it also raises significant unanswered questions about the scope of surveillance authorities and about implications for individual rights. In part, these questions arise because threats to U.S. national security have changed significantly over the last two decades. At the same time, the attention given to terrorism in our nation’s criminal laws has drawn new attention to the frequently overlapping missions of national security and law enforcement, and has threatened the theoretical bright line that law has traditionally drawn between national security and law enforcement surveillance.

In brief, electronic surveillance and physical searches may be conducted by agencies of the Intelligence Community in pursuit of foreign intelligence and foreign counter-intelligence information. Instead of the traditional law enforcement warrant requirements supplied by Title III of the Omnibus Crime Control and Safe Streets Act of 1968⁸ and Fourth Amendment case law, rules for national security investigations are found in the Foreign Intelligence Surveillance Act (FISA),⁹ in Executive Order 12,333¹⁰ and follow-on agency guidelines, and in the relatively uncharted confines of the Constitution.

To obtain ex parte authorization to conduct electronic surveillance of a “United States person” in the United States, the Attorney General must find and a judge of the FISC must be persuaded that there is probable cause that the target is an agent of a foreign power and that the acquisition of the foreign intelligence information sought is necessary to the national security. The FISC judge also must make one of four findings about the target:

1. that he knowingly engages in clandestine intelligence activities on behalf of a foreign power which “may involve” a criminal law violation.
2. that he knowingly engages in other secret activities on behalf of a foreign power pursuant to the direction of an intelligence network and his activities involve or are about to involve criminal violations.
3. that he knowingly engages in sabotage or international terrorism or is preparing for such activities, or
4. that he knowingly aids or abets another who acts in one of the above ways.

In addition, it must be shown that the intelligence cannot be obtained by less intrusive collection techniques. Finally, FISA requires that collecting agencies prescribe and follow procedures to minimize the acquisition, retention, and dissemination of information about U.S. persons who have not consented to surveillance.

Although Congress has asserted that Title III and FISA provide the exclusive means for conducting national security electronic surveillance,¹¹ no president has ever conceded the need for such authority, nor agreed that he is bound by its terms. In 1981, President Reagan issued Executive Order 12,333,¹² which supplies executive branch
rules for the conduct of intelligence activities by all U.S. agencies. It prohibits intelligence collection about U.S. persons except pursuant to rules approved by each agency head and by the Attorney General. Although the executive order directs that intelligence agencies “use the least intrusive”13 collection techniques in the U.S. or when directed at U.S. persons abroad, and forbids collecting information about the domestic activities of U.S. persons, it authorizes the Attorney General to apply for a secret warrant from the FISC if she determines “that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.”14

Beginning with George Washington, presidents have also authorized warrantless surveillance for national security purposes.15 Lower courts reviewing challenges to this practice have insisted that the surveillance be authorized by the President or the Attorney General, that the target be a foreign power or its agent, and that the primary purpose of the surveillance be to gather foreign intelligence information.16 It remains unclear in the Supreme Court, however, whether the substitution of FISA’s review process for the traditional warrant satisfies the Supreme Court’s first measure of the reasonableness of warrantless surveillance, namely, whether a target’s interest in privacy and free expression would be better served by a warrant requirement.17 However, the Court’s second test of reasonableness — whether the warrant requirement would “unduly frustrate the efforts of Government to protect itself”18— may be more easily met in the foreign intelligence setting.

Whatever the legal standards for conducting electronic surveillance, threats to our national security today are markedly different from those of a decade ago. The national security threat list, prepared by the Attorney General in cooperation with the FBI and Department of State, is intended to provide a strategy for national security intelligence gathering activities. The 1999/2000 version lists the major threats as: terrorism, espionage, proliferation, economic espionage, targeting the national information infrastructure, targeting the U.S. government, perception management, and foreign intelligence activities.19 In view of these changing threats, it is important to consider whether the rules codified in FISA, the executive order, and agency guidelines adequately assure adherence to the Supreme Court’s admonition that national security surveillance in the United States must be conducted in ways that “are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.”20

The February report also leaves several more particular intelligence collection questions unanswered. FISA, the executive order, and agency guidelines provide lesser protections for non-U.S. persons — those who are not citizens, permanent resident aliens, or U.S. corporations. Although the Supreme Court has held that the Fourth Amendment does not protect an alien with no substantial ties to the U.S. from otherwise unconstitutional searches by U.S. law enforcement agencies abroad,21 the Court has also held that “once an alien gains admission to our country and begins to develop ties that go with permanent residence his constitutional status changes accordingly.”22 Arguably, aliens lawfully in the U.S. should not categorically be denied the same protection from intrusive forms of surveillance in the United States that is afforded U.S. persons.

Second, FISA authorizes warrantless emergency orders for electronic surveillance or physical searches upon the decision of the Attorney General, while the executive order empowers the Attorney General alone to approve other forms of surveillance for which “a warrant would be required if undertaken for law enforcement purposes.” These authorities also provide for the classification of agencies’ procedures for the minimization of acquisition, retention, and dissemination of intelligence information. While these minimization requirements exist and are cited in the February report, their contents have not been subject to public scrutiny or to judicial review. The absence of an opportunity for public comment on minimization or a prior judicial check on these executive decisions may prevent enforcement of statutory and constitutional norms.

Third, FISA does not regulate U.S. agencies’ surveillance of U.S. persons abroad. The executive order authorizes the Attorney General alone to approve surveillance for intelligence purposes of a United States person abroad when the target is believed to be an agent of a foreign power. It is not clear what agencies are empowered to conduct such surveillance abroad, or whether foreign gov-

**Standing Committee on Law and National Security**

**Chair:** Elizabeth Rindskopf Parker


**Advisory Committee Chair:** Richard E. Friedman

**ABA Board of Governors Liaison:** James E. McDaniel

**Staff Director:** Holly Stewart McMahon; 740 15th St., NW; Washington, D.C. 20005-1009; (202) 662-1035; FAX: (202) 662-1032; E-mail: natsecurity@abanet.org; Web page: <http://www.abanet.org/natsecurity>
governments may be asked to conduct surveillance of U.S. persons abroad when U.S. agencies would not be authorized to do so. Nor is it clear that warrantless surveillance of U.S. persons abroad is constitutional, although some courts have approved it. Recognition of both international organized crime and international terrorism as threats to the U.S. national security makes these questions increasingly important.

Fourth, it is not clear that there is any legal authority other than Title III that empowers the U.S. to conduct electronic surveillance or a physical search for intelligence purposes of a target who has not been shown to be an agent of a foreign power, but who, alone or with others, may be planning a major terrorist assault in the U.S. Consider, for example, the next Timothy McVeigh.

Fifth, courts have held that the Title III warrant protections apply when the "primary purpose" of an investigation becomes law enforcement, rather than intelligence collection. The Aldrich Ames investigation shows the importance of separating intelligence collection from law enforcement, and of coordinating activities of the CIA and FBI in the U.S. As terrorist activities are increasingly criminalized, however, managing this "primary purpose" standard, or fashioning a new way to separate intelligence collection from law enforcement, will present a formidable challenge.

Finally, the recently released Report of the National Commission on Terrorism (Bremer Commission)24 blames a "lack of clarity" concerning FBI legal authority for a "risk-averse culture that causes some agents to refrain from taking prompt action against suspected terrorists."25 It also complains that Justice Department officials may require "evidence of wrongdoing or specific knowledge of the group’s terrorist intentions" in addition to foreign agency, before forwarding a request for FISA surveillance to the FISC. The Commission recommends development of a new guidance document to specify when FBI investigations of terrorism should be opened and to instruct field agents "to investigate terrorist activity vigorously, using the full extent of their authority."26 The problem, of course, is that agents are, at times, appropriately unsure of their authority. Drawing lines that permit intrusive surveillance for the purpose of collecting intelligence information when important privacy and expressive freedoms are at stake is not a simple task. In addition, agent uncertainty results from increasingly novel and complex nuances of new technology, along with changing permutations of foreign threats. National security surveillance presents a complex welter of questions, not sure-fire answers.


13 Exec. Order 12,333. § 2.4.

14 Id., § 2.5.


16 See Dycus et al., supra note 1, at 626-637.


18 Id.


20 Keith, 407 U.S. at 318.


23 United States v. Barona, 56 F. 3d 1087 (9th Cir. 1995).


25 Id. at 11.

26 Id.

Professor Banks is the Laura J. & L. Douglas Meredith Professor, Syracuse University College of Law, and Professor of Public Administration, Maxwell School of Citizenship and Public Affairs at Syracuse University. He is also the author of several books about national security and constitutional law.