Deterring Nuclear Terrorism

Michael A. Levi
Published in Issues in Science and Technology, Spring 2004.

Contrary to popular belief, with a little technological innovation deterrence can become a useful strategy against terrorist use of nuclear weapons.

Has terrorism made deterrence obsolete? President Bush articulated the prevailing view in his June 2002 West Point address: "Deterrence—the promise of massive retaliation against nations—means nothing against shadowy terrorist networks with no nation or citizens to defend. Containment is not possible when unbalanced dictators with weapons of mass destruction can deliver those weapons on missiles or secretly provide them to terrorist allies." Debate over missile defense aside, U.S. foreign policy thinkers have largely accepted his reasoning, though they argue on the margins over how unbalanced most dictators are.

Yet in confronting the prospect of nuclear terrorism—and there is no more dire threat facing America today—this logic is flawed. Its purported truth in addressing nuclear terror relies almost entirely on its assumption that rogue states could provide nuclear weapons "secretly" to terrorists. But were such now-secret links to be exposed, deterrence could largely be restored. The United States would threaten unacceptable retaliation were a state to provide the seeds of a terrorist nuclear attack; unable to use terrorists for clandestine delivery, rogue states would be returned to the grim reality of massive retaliation.

Most policymakers have assumed that exposing such links would be impossible. It is not. Building on scientific techniques developed during the Cold War, the United States stands a good chance of developing the tools needed to attribute terrorist nuclear attacks to their state sponsors. If it can put those tools in place and let its enemies know of their existence, deterrence could become one of the most valuable tools in the war on terror.

Terrorists cannot build nuclear weapons without first acquiring fissile materials—plutonium or highly-enriched uranium—from a state source. They might steal materials from poorly secured stockpiles in the former Soviet Union, but with the right investment in cooperative threat reduction, that possibility can be precluded. Alternatively, they could acquire fissile materials from a sympathetic, or desperate, state source. North Korea presented this threat most acutely when it threatened in May 2003 to sell plutonium to the highest bidder.

The Bush administration appears to be acutely aware of such a possibility and is trying to prevent it by fighting state-based nuclear proliferation and by attempting to eliminate terrorist groups. Yet it has taken few effective steps to break *direct* connections between terrorists and nuclear rogues. Elimination of terrorist networks and prevention of nuclear proliferation should be top goals, but a robust policy cannot be predicated on assuming universal success in those two endeavors.

Two basic lines of attack might help break any connection. In the one currently favored by the administration, militaries attempt to break the terrorist-state link physically by focusing on interdiction of nuclear weapons transfers. But the technical barriers to such a strategy's success are high. A grapefruit-sized ball of plutonium or a cantaloupe worth of highly-enriched uranium is enough for a crude nuclear weapon that would flatten much of a city, and detecting such a shipment would be extremely difficult. Like missile defense, interdiction is a useful tool in preventing nuclear attack, but also like missile defense, it is far from sufficient in itself. In

confronting the threat of missile attack, the United States ultimately relies on deterrence, threatening any would-be attacker with unacceptable punishment. It will need the same tool to prevent nuclear terrorism.

This, of course, begs a question: If nuclear materials are so hard to detect, how can state-terrorist connections be exposed? Solving this problem requires a novel and somewhat unsettling twist. Instead of simply focusing on intercepting bombs, we must learn to identify a nuclear weapon's origin *after* it has exploded by examining its residue. If the United States can take that technical step, it can credibly assure its enemies that their transfer of weapons to terrorists will ultimately lead to their demise.

At first glance, such a strategy might appear foolish: It would provide little comfort to identify an attack's perpetrator after a U.S. city has already been destroyed. Adopting this criticism, though, would miss the essence of deterrence. During the cold war, U.S. deterrence was based firmly in American ability to retaliate following a devastating Soviet attack. This by no means suggested that such an attack was acceptable, or that retaliation would provide comfort. Instead, what was important was the threat's ability to discourage any attack from occurring in the first place. Similarly, deterring nuclear terror by threatening its would-be sponsors would be aimed at using retribution not as an end, but as a means to preventing attacks.

The brightest line

Finding a successful deterrence strategy requires that we make retaliatory action as certain as possible; there must be little room for the adversary to gamble that it might transfer nuclear weapons without suffering. Ideally, the United States would identify nuclear transfers when they occurred and punish the participants accordingly. However, the difficulty of intercepting nuclear transfers might embolden enemies to attempt evading such a system. Moreover, enemies might believe that even if a transfer were detected, the United States would lack the resolve to punish them. Pyongyang, for example, with over ten thousand artillery pieces poised for counterattack against Seoul, might conclude that the United States would not follow through on its retaliatory threats were it to intercept a North Korean bomb that had not yet been detonated.

Focusing on actual attacks rather than on transfers would solve both of these problems. Few doubt the U.S. resolve to retaliate were a nuclear bomb to be detonated in a U.S. city. And unlike shadowy transfers of nuclear material, a nuclear attack would surely be noticed.

The missing link, which scientists must provide, is the ability to attribute a nuclear weapon to its state source *following* an attack. On its face, this might appear impossible—during a nuclear detonation, the weapon's fissile core of plutonium or uranium would be vaporized and transmuted, flung outward with the force of twenty-thousand tons of TNT. And yet surprisingly, such a cataclysmic event would still leave behind traces from which the original bomb's characteristics might be reconstructed.

Already, scientists at the nation's three principle nuclear weapons laboratories are working on the problem. They have decades of experience to build on. Before 1963, when the world ceased testing nuclear weapons in the atmosphere, the United States developed techniques to infer details of Soviet bombs by examining their fallout, which they could detect from far away. By positing a range of possible bomb designs, technicians could infer details about the fissile materials—plutonium or uranium—used in the Soviet bombs, along with some of the weapons' design details. (Presumably, the Soviets did the same to spy on the United States; thus, the two countries might cooperate to further develop attribution abilities.) Some of that expertise is still maintained, particularly in the conjunction with the Nuclear Emergency Search

Teams (NEST), whose task is to respond to nuclear terrorist incidents. Building on that foundation will require training a new generation of scientists in forensic techniques long-ago abandoned. It will also require an effort by laboratory scientists to imagine weapon designs terrorists or rogues might use. (Such designs could be simulated using the Department of Energy's Advanced Supercomputing Initiative and would not require nuclear testing to validate.) It would be wise to pursue much of this in a limited multilateral environment, thus helping reassure the world that our attributions are sound and unbiased.

By itself, however, the ability to infer a bomb's composition will not be enough. To successfully attribute an attack, there must be a state fingerprint to match it to. Knowing any characteristics of enemy weapons will be useful, but it will be particularly helpful to know the finer details of others' plutonium and uranium. Those two elements come in various isotopes, and a given sample of either metal will combine several of those isotopes in hard-to-alter combinations. To some degree, one can infer those characteristics from the design details of the enemy's production facilities and from the operating histories of its plants. In other cases, such as in Korea in the 1990s, special access will make it possible to measure the composition of a country's uranium or plutonium. If the isotopic details of a weapon are known, attributing it will be much easier.

It may be possible to go further by exploiting states' interest in not being wrongly identified as having originated a nuclear attack. In conjunction with strengthened International Atomic Energy Agency safeguards, states could be required to submit detailed isotopic data on the nuclear materials they produce and to submit to its verification. If such states had pure intentions, this would help exclude them from blame were a future terrorist attack to occur; were their motives more suspect, this would provide the world a hedge against their future breakout. So far, states have been loathe to take such actions, as they could require compromising sensitive military and commercial data. But the tradeoffs in confronting terrorism—in particular, in the immediate aftermath of an attack—might prompt many to reconsider.

Ambiguous intent

Physical identification of bombs with their builders still leaves open the question of intent. Imagine that a bomb made of North Korean plutonium were detonated in Washington: Would it not be essential, some ask, that we know the plutonium had been provided to terrorists intentionally, rather than stolen against the regime's wishes? In fact, it should not matter. Instead, in deciding whether it would be appropriate to retaliate for an attack, we must ask two questions: Is it morally acceptable to retaliate? And is it strategically wise?

Insofar as deterrence itself is morally acceptable (a controversial proposition in some circles, but one at least tacitly accepted in the strategies of all eight nuclear powers), the threat and act of retaliation against an enemy for leaking nuclear materials, whether intentional or otherwise, is moral too. With possession of nuclear weapons comes the responsibility for their control. If a state is unwilling to accept responsibility for the impact of any weapons it builds, it can choose not to build them. By foregoing that choice, it should be understood that the state takes responsibility for any impact the weapons have. To see that such a proposition is widely accepted, one need look no further than the cold war, where deterrent threats made little or no distinction between intentional and accidental launches of Soviet or U.S. missiles.

The strategic wisdom of retaliation under ambiguous circumstances is another matter entirely. Against an attack originating from North Korea or Iran, whether intentional or not, there would be little for the United States to lose were it to retaliate. Since the result of the

retaliation would likely be regime change, it would be effective in removing the nuclear threat. Ideally, that prospect would induce both regimes not only to refrain from exporting nuclear materials, but also to secure their stockpiles.

In contrast, were an attack to originate from loose Russian material, military retaliation would be unwise. It is currently inconceivable that such an attack would be intentional on Russia's part, as Russia is not an enemy; moreover, retaliation would do little to prevent further leakage of Russian material, and indeed might provoke Russian retaliation in kind. The precedent for such an approach is also found in the changed U.S. attitude toward accidental missile launch since the cold war. Does anyone believe that it would be strategically wise for the United States to retaliate militarily against an (improbable) accidental launch of a Russian missile?

Perhaps the toughest case is Pakistan, currently an ally in the war on terrorism. Few U.S. policymakers are confident that Pakistan's nuclear arsenal is entirely secure, making weapons-theft by terrorists a distinct possibility. At the same time, many doubt the sincerity of Pakistan's cooperation with the United States, and given its past sales of nuclear equipment to North Korea, Iran, and Libya, there would likely be doubts as to whether nuclear material leaked from Pakistan was proliferated intentionally or was stolen. U.S. policy towards Pakistan on this question will likely depend on how the broader U.S.-Pakistani relationship evolves. President Bush's national security team needs to debate now how it would respond to a leak of Pakistani nuclear material. If it concludes that it will hold the Pakistani regime responsible for any nuclear leaks, it should communicate its decisions clearly, though quietly, to the Pakistani leadership. At the same time, it should offer to help Pakistan secure its arsenal against theft.

Last year, a National Research Council panel, in addressing the threat of nuclear terrorism, reported that "The technology for developing the needed attribution capability exists but has to be assembled." It noted that an effort to complete that work is under way in the Pentagon's Defense Threat Reduction Agency, but that it is not expected to be complete for several years. If attribution is construed merely as something useful after an attack, perhaps to provide evidence in prosecuting the offenders, it makes sense for it to take a back seat to urgent efforts such as securing ports and improving surveillance. Attribution, however, has the potential to be far more powerful. Coupled with the right threats, it can prevent terrorist attacks in the first place. The scientific effort must be accelerated, and declaratory policy must be modified to match.

Michael Levi (mlevi@brookings.edu), a physicist, is the science and technology policy fellow in foreign policy studies at the Brookings Institution.

Recommended reading

Jay C. Davis, "The Attribution of WMD Events," *Journal of Homeland Security*, April 2003

National Academies of Sciences, *Making the Nation Safer*, Chapter 2 (Washington, D.C.: National Academies Press, 2002).