Caitlin Talmadge

Deterring a Nuclear 9/11

Can the United States deter a nuclear terrorist attack? Two conventional wisdoms prevail on this question. One contends that Cold War ideas about deterrence are utterly irrelevant to coping with an enemy such as al Qaeda, whose members are unafraid of earthly punishments and whose leaders lack a return address at which to direct retaliation.[1] The other suggests, more optimistically, that nuclear forensics make it possible for the United States to determine the origin of nuclear bombs and thus credibly threaten retaliation against any state that transfers nuclear material, weapons, or knowledge to terrorists.[2] Following this logic, the United States need only combine modern nuclear physics with concepts of deterrence honed in the Cold War to solve its most worrisome present-day threat.

Both arguments are half correct. Deterring a suicidal, transnational terrorist enemy is a dubious proposition and by itself hardly a comforting strategy for protecting the country. Nevertheless, nuclear terrorism is not like other forms of terrorism because states have to be involved at some stage in the decision chain leading to this type of attack. It is possible to deter nuclear terrorism by threatening retaliation against regimes or military establishments that either deliberately transfer nuclear materials, weapons, or knowledge to terrorists, as North Korea might do, or that turn a blind eye to substate organizations or actors engaged in such activities, as Pakistan did when the father of its nuclear program, A. Q. Khan, began to sell secrets.[3] Engaging in what Robert Gal-

Caitlin Talmadge is a doctoral candidate and member of the Security Studies Program in the Department of Political Science at the Massachusetts Institute of Technology. In preparing this article, she benefited from the advice of Charles Ferguson, Brendan Green, Stephanie Kaplan, Steven Lehotsky, Jon Lindsay, Austin Long, Andrew Marshall, Whitney Raas, Steve Rosen, James Schlesinger, Paul Staniland, and other individuals who did not wish to be thanked by name.

The Washington Quarterly • 30:2 pp. 21–34.

lucci has called "expanded deterrence" against these actors, however, depends not only on developing appropriate nuclear forensic techniques but also on overcoming important strategic, political, diplomatic, and organizational challenges that have yet to garner sufficient attention from those who invoke the Cold War legacy of deterrence.[4]

Deterrence Theory Revisited

Classical deterrence theory is a product of the Cold War, a period in which the superpowers' vast nuclear arsenals made it imperative to avoid direct conflict. Thomas Schelling, writing in an era of nascent strategic parity between the United States and the Soviet Union, defined deterrence as "persuading a potential enemy that he should in his own interest avoid certain courses of activity."[5] According to Schelling, deterrence worked by convincing the enemy that the costs of taking some action outweighed the benefits. Whether the enemy was convinced or not would depend on the credibility of the threats made against him.

It is possible to deter nuclear terrorism.

As other theorists later observed, credibility depends on whether the country making threats has the ability to carry them out and an interest in doing so.[6] In short, military capabilities alone do not confer deterrent power. For a threat to be effective, those capabilities have to be combined with communication about the interests at stake and how military capabilities would be used to serve those interests.

As Schelling noted, deterrence "involves confronting [the enemy] with evidence that our behavior will be determined by his behavior."[7] To the extent that the United States could make itself appear irreversibly committed to carrying out its threats in the event that the enemy took a proscribed action, its deterrent would be more effective. Conversely, however, the object of the threat also had to be convinced that he would avoid the feared consequences by refraining from the proscribed behavior. Deterrence required reassurance. If an opponent believed he would suffer the consequences regardless, then he had little incentive to alter his behavior.[8]

Glenn Snyder usefully divided deterrence into two types: deterrence by punishment and deterrence by denial.[9] Deterrence by punishment threatened to impose costs on the adversary if he committed a proscribed action. For example, during the Cold War the United States tried to deter the Soviet Union by making it clear that an attack on New York would be met with an attack on Moscow. Deterrence by denial threatened to reduce the benefits that an adversary could expect to gain from committing a proscribed action. This form

of deterrence usually involved defensive efforts or shows of resolve. During the Cold War, for example, the United States built missile defenses partly in an attempt to convince the Soviet Union that a first strike would not achieve its goals, and it created an immense military presence in Western Europe as a way of displaying its intention to defend the territory from Soviet attack.

Through these sorts of policies, the United States and Soviet Union managed to deter each other for more than 40 years. Although few ever felt truly comfortable with the concept of mutually assured destruction, deterrence emerged from the Cold War with a vaunted reputation for having helped to avert a nuclear exchange.

Deterrence Theory Restored

The end of the Cold War, the rise of transnational terrorism, and the devastating attacks of September 11, 2001, led many to see deterrence as passé. It was said no longer to apply because terrorists are irrational fanatics who seek martyrdom and/or because they lack return addresses. The 2002 National Security Strategy stated outright that "[t]raditional concepts of deterrence will not work against a terrorist enemy whose avowed tactics are wanton destruction and the targeting of innocents; whose so-called soldiers seek martyrdom in death and whose most potent protection is statelessness."[10] Richard Betts enunciated a similar logic, concluding that "both deterrence and defense are weaker strategies against terrorists than they were against communists."[11] Even a recent study that identified strategies for deterring terrorism, such as threatening to intervene in local political conflicts of concern to terrorists and their supporters, conceded that this strategy would have little utility against a highly motivated transnational group such as al Qaeda.[12]

These analysts have in effect urged the United States to focus on deterrence by denial: massive investment in homeland security to convince individual terrorists that their efforts to attack the United States will be fruitless. Few really believe, however, that homeland security serves a deterrent function. No matter the level of protection, a creative and determined terrorist is likely to believe, correctly, that he can find some way to attack. His means are nearly limitless, and he need kill only a few people to frighten many more.

Because terrorists lack return addresses, analysts have dismissed even more firmly the possibility of deterrence by punishment, or the threat to impose unbearable costs on those who would do the United States harm. This disheartening conclusion stems from a failure to appreciate the many steps terrorists must take before committing an actual attack. Many of these steps depend on assistance from people and organizations that may not be as impervious to deterrence by punishment as individual terrorists are. If the United States can

broaden the range of actors it seeks to deter and convince these other actors that cooperating with terrorists is not in their interests, it may be able to reduce the likelihood of a terrorist attack substantially.[13]

Nowhere is this approach more plausible than in the case of nuclear terrorism.[14] Unlike other forms of terrorism in which terrorists are more or less self-sufficient, it is virtually impossible for terrorists to create their own nuclear material, regardless of which ingredient they use. Producing plutonium requires sophisticated, expensive reactors, as well as reprocessing facilities. Enriching uranium to a weapons-grade level can be done through several techniques; all require relatively large buildings and advanced technologies.[15] Both paths to nuclear material require a sizable and scientifically knowledgeable labor force, significant industrial resources, and time. Weapons design and delivery pose additional obstacles. States such as Argentina, Iran, Iraq, and Libya have tried to produce nuclear weapons and failed. Aum Shinrikyo, one of the best-funded terrorists groups in history and instigator of the 1995 sarin gas attacks in Tokyo, was also unable to create its own nuclear material and had to attempt to buy it from Russia.[16]

It is virtually impossible for terrorists to create their own nuclear material.

As such, it is extremely likely that states or substate military organizations would have to be involved in the tacit or overt provision of nuclear material to terrorists. A state could directly and deliberately transfer a weapon or materials to terrorists. It could refuse to halt or punish those in the military or scientific community who sell material or weapons to terrorists. It could willfully neglect nuclear security or choose not to alert the international community to suspected thefts of material or weapons. It could turn a blind eye to terrorist activities occurring on its territory.

In all of these cases, the United States does have a target against which it can direct threats of retaliation: the governments or military and scientific establishments that actively or passively assist aspiring nuclear terrorists. Even if the United States cannot deter individual terrorists, it can create strong incentives for these other actors to block terrorist acquisition of the ingredients required for a nuclear attack. They have addresses, lives, and property that the United States can hold hostage to their wholehearted cooperation. As Paul Davis and Brian Jenkins of RAND have argued, "The United States could announce credibly that … it would punish not only active supporters, but even those states and factions that merely tolerate the terrorists or indirectly facilitate their acquisition of [weapons of mass destruction (WMD)]. The purpose would be to so alarm heads of state and heads of substate organi-

zations that they would work actively to get rid of elements that might bring destruction down upon them."[17]

Bush threatened as much after the North Korean test, warning that the United States would hold the regime "fully accountable" if it passed nuclear materials or weapons to terrorists.[18] The 2006 version of the U.S. National Security Strategy reflects a similar logic, suggesting a subtle shift from the 2002 document. In describing "a new deterrence calculus," the current strategy declares, "States that harbor and assist terrorists are as guilty as the terrorists, and they will be held to account." That document, along with analysts such as Gallucci who argue that a form of "expanded deterrence" against nuclear terrorism is possible, points to the crucial importance of being able to "define the nature and source of a terrorist-employed WMD. Should a WMD terrorist attack occur, the rapid identification of the source and perpetrator of an attack will enable our response efforts and may be critical in disrupting follow-on attacks."[19]

In other words, nuclear forensics is the linchpin of any attempt at a deterrence-by-punishment strategy against governments, militaries, or other organizations that might actively or passively assist terrorists in a nuclear attack on the United States.[20] Although forensics is the first step toward making credible threats of retaliation against these actors, using it as the basis of a new deterrence posture will require solving a related series of strategic as well as political challenges and will necessitate careful consideration of the countermeasures terrorists may take in response.

A Primer on Nuclear Attribution

Nuclear attribution is the process of identifying the source of nuclear or radioactive material. It involves integrating multiple forms of nuclear forensic information with other intelligence and traditional investigative work.[21] Nuclear forensics is possible because weapons-grade materials do not occur naturally in quantities large enough to make weapons. Natural uranium contains only 0.7 percent U-235; it must be enriched to at least 20 percent U-235 in order to become fissile and to 90 percent to become bomb-grade. Similarly, plutonium exists naturally only in trace amounts; nuclear reactors are needed to produce quantities of Pu-239 large enough to make a weapon, and even then varying trace amounts of Pu-240 remain. Because of these basic facts, the choice of one material over the other and the processes used to make that material weapons-grade reveal clues about the origins of the weapon itself.

As such, every weapon has signatures—physical, chemical, elemental, and isotopic properties that reveal something about what the weapon contained and how it was made. For example, physical signatures would depend on the nuclear material's texture, size, and shape, while chemical signatures

would come from its unique molecular components.[22] Different reprocessing techniques also leave behind trace amounts of certain organic compounds or elements that then point to particular technical approaches used. Isotopic signatures of the material can "indicate that the material has been in a nuclear reactor and serve as a fingerprint for the type and operating conditions of a given reactor."[23] They can also help determine the material's age, providing further clues about its origins.

In combination, these various signatures may help narrow the type of reactor from which the plutonium came or suggest the enrichment process used to make the uranium. When compared against a database of known reactor types or a sample of known highly enriched uranium stockpiles, it may become possible to determine the material's origins or at least to exclude certain sources and then identify the culprit through a process of elimination when combined with other intelligence and data about the situation.[24]

Nuclear forensics is the linchpin of any attempt at deterrence by punishment.

Additionally, analyzing the airborne debris left after a nuclear explosion, known as fallout, can help the forensic analyst estimate the efficiency of the bomb design, which in turn can help reveal who might have built it.[25] Modern thermonuclear weapons have a higher efficiency than the sort of first-generation nuclear weapons used at Hiroshima and Nagasaki. Existing computer programs can help estimate the predetonation isotopic mixture, which, combined with analysis of the postdetonation isotopic mixture, may make it possible to infer the bomb's efficiency and thus its design.[26] The bomb design can further narrow the possible origins of the weapon. It is extremely implausible that a terrorist group would be able to construct a thermonuclear (hydrogen) or boosted implosion (tritium and deuterium) bomb on its own without state assistance. If the forensic analysis suggested this sort of bomb, it would be clear either that the weapon was stolen from a state's poorly secured stockpiles or that a state directly assisted the terrorist group in assembling it. Meanwhile, a crude, gun-type uranium device with a relatively low efficiency would more likely point to terrorist construction.

The United States' Nuclear Emergency Search Team also maintains a database of known weapons designs against which these findings could be compared.[27] Forensic analysts could examine debris to "find traces of bomb components such as the casing, the reflector, and the conventional high explosive" that would provide further clues about the construction process.[28] As such, nuclear forensics does have the potential to provide a number of clues that might help to narrow down the origin of a bomb. Yet, clues are

just that; they alone cannot necessarily identify the culprit in the absence of other intelligence.

Current U.S. Attribution Capabilities

The United States developed considerable attribution capabilities during the early Cold War period in an effort to determine the size, type, and location of Soviet nuclear tests.[29] This research largely stagnated after aboveground nuclear tests went out of style in the 1960s, and today few scientists are trained in nuclear forensic techniques.[30] The United States retains a lone aerial collection aircraft from that era, the WC-135W Constant Phoenix, recently deployed to "sniff out" radiation in the aftermath of the North Korean nuclear test.[31] In the future, the United States may want to acquire additional specialized aircraft, equipped with air-sampling devices that operate like vacuums to suck in particles as the aircraft crosses paths with a nuclear plume. Sandia National Laboratories has begun development of improved sensors to place on board this sort of aircraft. Robots or other unmanned vehicles may be able to do some of this work as well.

In 2002 the Pentagon established a team of forensic analysts to improve the country's nuclear attribution capabilities. This team, in combination with the ongoing research at the national labs, is promising. It claims to have forged an "initial integrated operational capability for rapid and accurate attribution."[32] The current National Security Strategy obliquely refers to these efforts, stating, "We will ensure that our capacity to determine the source of any attack is well-known, and that our determination to respond overwhelmingly to any attack is never in doubt."[33]

Many technical experts nevertheless remain less than optimistic about the current U.S. capability to identify the origin of a terrorist nuclear weapon. The problem is not just technical but also organizational. Noticeably, there is still no single institution with responsibility for nuclear attribution. In late 2006, the Department of Homeland Security did launch the National Technical Nuclear Forensics Center in an attempt to integrate national capabilities across interagency lines in this area.[34] Work, however, is still spread across the Departments of Energy, State, Defense, and Justice as well as eight national laboratories. As Jay Davis, former director of the Defense Threat Reduction Agency, has noted, "We in fact have many of the technical and operational tools we need, but they have not been focused on the issue of terrorism and its associated forensics and attribution needs along event timelines. These tools may not easily reconfigure across organizational and authority boundaries."[35]

Additionally, the officials who must orchestrate the political and diplomatic aspects of any deterrence policy may not have considered how to evaluate

technical uncertainties inherent to the attribution process. The advent of fingerprinting and, later, the discovery of DNA forced the criminal justice system to decide what sorts of standards such evidence had to meet to form the basis for determinations of guilt or innocence. This decision was for those in the courtroom, however, not just those in the crime laboratory. Likewise, with the advent of improved nuclear forensics, leaders outside the technical community will have to participate in the process of setting some standards about what types of evidence will justify which sorts of U.S. retaliation. Technical experts could disagree on how to interpret forensic evidence just as two expert witnesses might look at the same fingerprint and assign different levels of probability to a proposed match. The technical, policy, and operational communities will have to unite to consider and resolve these potential problems.

Political leaders also must understand that it is extremely unlikely that the United States would be able to identify the origin of a detonated nuclear weapon based on technical information alone, as those who advocate crash programs in forensics have sometimes implied. Political leaders making decisions about retaliation would need to corroborate any technical findings with other intelligence, such as evidence that terrorists had recently traveled to the country from which the nuclear material was believed to have originated.

Ironically, the intelligence is likely to be best in cases where the United States is least interested in retaliating. The United States is likely to have the best intelligence about the arsenals, behavior, and intentions of its allies, such as the United Kingdom and Israel, who also are the least likely to have provided either passive or active assistance to terrorists and against whom retaliation would be inconceivable. The United States is likely to have the least reliable corroborating intelligence in regard to the countries it would mostly deeply suspect of actively or passively assisting terrorists, such as Iran, North Korea, and Pakistan. This conundrum greatly complicates the attempt to turn nuclear forensics, a set of technical findings, into an attribution capability that could underlie credible threats of retribution.

Attribution Requires International Cooperation

Attribution also depends fundamentally on a database against which to compare the information discovered in the forensic process. Identifying the signatures of any particular weapon is of little value in itself if the United States lacks information on the signatures of other weapons and supplies of fissile material worldwide. Some databases already exist through the Nuclear Smuggling International Technical Working Group (ITWG), formed to assist in predetonation forensic analysis of smuggled nuclear material.[36] The ITWG is also developing a set of standardized methods that can be used to handle

samples of fissile material and to perform forensic tests.[37] For its part, the United States has been working since at least the mid-1990s to establish an even larger international database of nuclear and radiological materials.[38] It is not clear that any of these databases are configured in such a way as to facilitate rapid analysis in the aftermath of an attack.

Additionally, the databases are incomplete. The United States should focus in particular on compelling cooperation from China, India, Israel, North Korea, and Pakistan, who have resisted participation. The United States may want to emphasize that it considers countries that do not provide samples for the databases to be admitting that they have not ruled out a clandestine attack on the United States through a terrorist intermediary. States that are serious about keeping their material and weapons from terrorists will have little to fear from contributing to the database. Indeed, they stand to benefit if they themselves are attacked or by being quickly ruled out in the event of an attack on another state. The United States should issue a standing invitation to assist states wishing to provide information relevant to the attribution process and to states needing assistance in securing their weapons and materials. It could also encourage states to "tag" their nuclear materials by making small but uniquely identifiable changes to the isotopic mixtures used in weapons.[39]

> There is still no single U.S. institution with responsibility for nuclear attribution.

Gallucci has suggested that the United States could grease the wheels of this process by sharing its own signatures as a sign of good faith.[40] With the same goal in mind, other experts have proposed that the database housing such material "would need to avoid any suspicion of political bias by conducting chemical and physical analyses in several laboratories in different countries under the international auspices of a body such as the [International Atomic Energy Agency]."[41] Concerns about such bias may be particularly acute in light of recent U.S. intelligence failures. For now, however, the United States appears to be pursuing a more unilateral approach to building a database, including potentially gathering samples covertly in foreign countries.[42] There are no signs that it plans to share its own signatures.

From Attribution to Deterrence

Even once the United States develops appropriate forensic techniques, acquires the assets needed for fallout collection and forensic analysis, and gathers enough information from other countries to engage in a plausible process

of elimination after an attack, the deterrent value of any resulting attributing capability is far from assured.

Deterrence will depend on convincing other states and even skeptics in the U.S. government that the United States actually has the ability to identify the origins of a nuclear weapon detonated on its soil. The United States could exaggerate this capability in an attempt to deceive its adversaries, and it might want to do so in the short to medium term.[43] Ultimately, however, the most persuasive means of convincing the world of a U.S. attribution capability is actually to have one and then to publicize it. Some avenues for such discussion are obvious: national strategy documents, presidential or other high-level statements, and strategically placed media leaks. Other opportunities would be more subtle: encouraging members of the U.S. scientific community to disseminate credible information to their colleagues overseas, emphasizing the capability in bilateral or multilateral talks with countries of concern, and using third parties to convey the information through diplomatic back channels. Whatever the approach, the United States would want to send a credible, recurring message that it could and would find a return address for any nuclear bomb.

U.S. leaders also would want to emphasize that retaliation, perhaps in kind, perhaps through devastatingly precise conventional attacks, would be strategically necessary and politically unavoidable in the aftermath of a terrorist nuclear detonation. The U.S. government could not sit idly by, knowing the origin of a terrorist nuclear weapon detonated on its soil, and not retaliate against the state(s) or substate organization(s) responsible for it, especially if those states or organizations had a history of supporting terrorism. To do otherwise would be to invite follow-on attacks and to allow the deaths of hundreds of thousands of Americans to go unanswered. The American public would demand retribution, especially if the terrorists themselves were nowhere to be found.

Or so U.S. leaders could claim, whether it is true now or not. The more that U.S. leaders publicly emphasize the possession of an attribution capability and a willingness to retaliate against those who assist terrorists, the more the public will in fact expect such retaliation. The more that other countries sense this domestic expectation, for instance, in polling data that the U.S. government might want to disseminate, the more politically credible the U.S. threat to retaliate in such cases will seem. This credibility will ultimately strengthen deterrence, making it plain that U.S. leaders would have little choice but to wreak destruction on governments, militaries, or other substate organizations that are found to have assisted aspiring nuclear terrorists.

Still, the United States must act with caution. In communicating its augmented attribution capability, the United States must strike a balance between providing enough information to be credible and providing so much information that adversaries can devise countermeasures. In this regard, nuclear attribution

presents a classic dilemma of deterrence, not unlike those of the Cold War. In that era, the United States advertised some of the capabilities it was developing for conflict with the Soviets while it hid others. Washington announced the intention to develop missile defenses long before the technology was ready, for example, because even the prospect of this weapons system had the potential to convince the Soviets that they could not win the strategic arms race. The United States hid other capabilities, such as stealth aircraft, until they were actually deployed, fearing that if the Soviets learned too much too soon, they would counter the innovation. Likewise, the more terrorists or collaborating states understand about the specific forensic techniques the United States favors, the more they may adjust their choices of nuclear material and bomb designs accordingly. U.S. statements should say as much as possible about what the United States can do while revealing as little as possible about how it can do it.

If too much information is released, terrorists could take dangerous countermeasures.

Well-publicized exercises are one of the best ways to demonstrate capabilities and a willingness to use them while controlling exactly which technical or operational details are released. The United States has used this approach in other areas, such as the Proliferation Security Initiative (PSI). PSI members conduct periodic, mock ship boardings and other exercises, and the participating governments issue press releases in order to remind the international community that the capability and intent to perform interdictions continues. Although the occurrence of these exercises is always reported, projecting an image of continued commitment to the PSI and growing interdiction capabilities, no information is released that could assist the targets of the PSI in evading interdiction.

The Department of Homeland Security takes a similar approach with its annual TOPOFF exercises that bring together top officials from federal, local, and state organizations to practice how to respond to various types of national emergencies. Although the press always reports the exercises' general parameters and their outcomes, media accounts studiously avoid any mention of exactly how the participants overcame the exercise's challenges.[44] Exercises in nuclear attribution could be handled similarly, greatly enhancing the capability's deterrent value while carefully controlling the information released.

If too much information is released, terrorists could take dangerous countermeasures. They could intentionally choose material or a bomb design that fools the United States into assigning responsibility to the incorrect party or clouds the U.S. ability to assign any responsibility at all. An overly rigid deterrence policy could also encourage one state to attempt to make a bomb ap-

pear as though it originated from a different state, in an effort to ignite a U.S. conflict with that other state. The belief that the United States could trace nuclear material back to a pariah regime might stimulate terrorists to set their sights on nuclear material in Europe instead. Of course, such a scenario is a reason to secure nuclear material in Europe.

Political leaders must understand the technical limitations of forensic analysis.

Nevertheless, these sorts of problems underscore why political leaders must understand the technical limitations of forensic analysis well enough to make credibly nuanced threats of retaliation. They also show why any serious attribution effort must be part of a broader campaign to secure all supplies of nuclear material worldwide, so that if a nuclear bomb goes off, the list of potential sources of fissile material is as short as possible.

Deterring a Nuclear 9/11

If the United States develops a credible nuclear attribution capability, states that wish to protect their citizens, territory, and interests are more likely to refrain from providing assistance to terrorists in the first place. Some might even find that they have a newly discovered interest in securing their nuclear materials, weapons, or expertise. It is difficult to imagine that the Pakistani government would turn a blind eye to a future A. Q. Khan if it believed that nuclear material or technology could be traced definitively back to Pakistan and that its people and infrastructure would suffer the consequences if those items were used in an attack against the United States. A similar logic might caution Iran against transferring such items to Hizballah, a long-standing recipient of conventional Iranian military technology and armaments, or warn North Korea against selling parts of its emerging nuclear arsenal to the highest bidder.

Still, deterring this sort of attack is neither as impossible nor as simple as most analysts have argued. The United States should invest heavily in an augmented attribution capability, which does hold the power to help deter states from providing crucial passive or active assistance to aspiring nuclear terrorists. Nuclear forensics also offers the morally comforting prospect that the United States can avoid wantonly retaliating against innocent parties, just as DNA reduced the risk of executing an innocent defendant. Yet, here, as in the courtroom, users have to be aware of the potential limitations of this new form of evidence and to develop rules governing its use. Forensics does not work in a vacuum or provide a technical solution to what remain fundamentally strategic, political, and organizational problems.

Notes

1. Richard K. Betts, "The Soft Underbelly of American Primacy: Tactical Advantages of Terror," *Political Science Quarterly* 117, no. 1 (2002): 31.
2. Graham Allison, "Deterring Kim Jong Il," *Washington Post*, October 27, 2006, p. A23.
3. Bill Powell and Tim McGirk, "The Man Who Sold the Bomb," *Time*, February 14, 2005, pp. 23–31.
4. Robert L. Gallucci, "Averting Nuclear Catastrophe," *Harvard International Review* 26, no. 4 (Winter 2005), http://hir.harvard.edu/articles/1303/.
5. Thomas Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard University Press, 1960), p. 9.
6. Daryl Press, "The Credibility of Power: Assessing Threats During the 'Appeasement' Crises of the 1930s," *International Security* 29, no. 3 (Winter 2004–05): 136–169.
7. Schelling, *Strategy of Conflict*, p. 13.
8. Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), chaps. 2 and 3; Thomas J. Christensen, "The Contemporary Security Dilemma: Deterring a Taiwan Conflict," *The Washington Quarterly* 25, no. 4 (Autumn 2002): 7–21.
9. Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, N.J.: Princeton University Press, 1961).
10. "The National Security Strategy of the United States of America," September 2002, chap. 5, http://www.whitehouse.gov/nsc/nss/2002/nss5.html.
11. Betts, "Soft Underbelly of American Primacy," p. 31.
12. Robert F. Trager and Dessislava P. Zagorcheva, "Deterring Terrorism: It Can Be Done," *International Security* 30, no. 3 (Winter 2005–06): 105–106, 122.
13. Michael J. Powers, "Deterring Terrorism With CBRN Weapons: Developing a Conceptual Framework," *CBACI Occasional Paper*, no. 2 (February 2001), pp. 5, 7, https://www.hsdl.org/homesec/docs/nonprof/nps08-091704-01.pdf.
14. Robert L. Gallucci, "Averting Nuclear Catastrophe: Contemplating Extreme Responses to U.S. Vulnerability," *Annals of the American Academy of Political and Social Science*, no. 607 (September 2006): 57–58; David Ignatius, "We Need a New Deterrent," *Washington Post*, October 11, 2006, p. A19 (quoting Graham Allison).
15. Richard Rhodes, *The Making of the Atomic Bomb* (New York: Simon & Schuster, 1988).
16. Jessica Stern, *The Ultimate Terrorists* (Cambridge, Mass.: Harvard University Press, 1999), pp. 64–65.
17. Paul K. Davis and Brian M. Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda* (Santa Monica, Calif.: RAND, 2002), p. 40.
18. Tanalee Smith, "Bush Warns North Korea Against Nuclear Proliferation," Associated Press Worldstream, November 16, 2006.
19. "National Security Strategy of the United States of America," March 2006, sec. 5, http://www.whitehouse.gov/nsc/nss/2006/sectionV.html (hereinafter 2006 National Security Strategy).
20. Graham Allison, "Making Good on Bush's Vow Will Require Detective Work," *New York Times*, October 13, 2006, p. 12.
21. "Nuclear Forensics Support," *IAEA Nuclear Security Series*, no. 2 (2006): 10. For the best textbook on this subject, see Kenton J. Moody, Ian D. Hutcheon, and Patrick M. Grant, *Nuclear Forensic Analysis* (New York: Taylor & Francis, 2005).

22. For this and all subsequent examples in the paragraph, see "Nuclear Forensics Support," p. 30.
23. Ibid.
24. Jay Davis, "The Attribution of WMD Events," *Journal of Homeland Security*, April 2003, http://www.homelandsecurity.org/journal/Articles/davis.html.
25. Dwight L. Williams, "Characterizing Nuclear Weapons Explosions Based Upon Collected Radionuclide Effluents," memorandum, MIT Department of Nuclear Science and Engineering, October 21, 2006.
26. Charles D. Ferguson, "Can Nuclear Forensics Trace a Detonated Nuclear Weapon to Its Source?" (working paper, American Political Science Association Conference, August 31, 2006), http://64.112.226.77/one/prol/prol01/index.php?cmd=Download+Document&key=unpublished_manuscript&file_index=1&pop_up=true&no_click_key=true&attachment_style=attachment&PHPSESSID=20a7317a3c52a7cf6f77a07e959a053c.
27. Jeffrey T. Richelson, "Defusing Nuclear Terror," *Bulletin of the Atomic Scientists* 58, no. 2 (March/April 2002), http://www.thebulletin.org/print.php?art_ofn=ma02richelson.
28. Ferguson, "Can Nuclear Forensics Trace a Detonated Nuclear Weapon to Its Source?"
29. Jeffrey T. Richelson, *Spying on the Bomb: American Nuclear Intelligence From Nazi Germany to Iran and North Korea* (New York: W.W. Norton, 2006), pp. 77–87.
30. Michael Levi, "Deterring Nuclear Terrorism," *Issues in Science & Technology* 20, no. 3 (Spring 2004), http://www.issues.org/20.3/levi.html.
31. William Broad and Mark Mazzetti, "Small Blast May Be Only Partial Success, Experts Say," *New York Times*, October 10, 2006, p. A8; Bryan Bender, "Pentagon Hunting for Clues on Power, Makeup of Weapon," *Boston Globe*, October 10, 2006, p. A1.
32. William Broad, "New Team Plans to Identify Nuclear Attackers," *New York Times*, February 2, 2006, p. 17.
33. 2006 National Security Strategy, sec. 5.
34. Department of Homeland Security Press Office, "U.S. Department of Homeland Security Addresses the Technical Nuclear Forensics Mission With the National Technical Nuclear Forensics Center," October 19, 2006.
35. Davis, "Attribution of WMD Events."
36. "Nuclear Forensics Support," p. 10.
37. Michael May et al., "Preparing for the Worst," *Nature*, October 26, 2006, pp. 907–908.
38. Ferguson, "Can Nuclear Forensics Trace a Detonated Nuclear Weapon to Its Source?"
39 . P. Gilfoyle and J. A. Parmentola, "Using Nuclear Materials to Prevent Proliferation," *Science and Global Security* 9, no. 2 (2001): 81–92.
40. Gallucci, "Averting Nuclear Catastrophe," p. 57.
41. May, "Preparing for the Worst," p. 907.
42. "U.S. Creates Nuclear Forensics Center," *Defense News*, October 23, 2006, p. 1.
43. See National Defense University Center for Counterproliferation Research, "At the Crossroads: Counterproliferation and National Security Strategy," April 2004, p. 37.
44. "U.S. Department of Homeland Security Announces Completion of Topoff 4 Command Post Exercise," States News Service, June 22, 2006.