Testimony of

Dr. Michael A. Levi

July 27, 2006

Prepared Statement of
Michael A. Levi
Fellow for Science and Technology, Council on Foreign Relations
Before the Committee on the Judiciary
Subcommittee on Terrorism, Technology, and Homeland Security
United States Senate
July 27, 2006

Chairman Kyl, Senator Feinstein, thank you for inviting me to speak with you about U.S. efforts to detect smuggled nuclear weapons. Current programs to enhance detection of smuggled nuclear weapons are, despite some important flaws, making valuable contributions to national security. They are not, and will never be, the most powerful means of defense - that role falls to programs that secure nuclear weapons and materials at the source. But assessed in the context of a much broader system aimed at reducing the likelihood of catastrophic nuclear attack, and judged against the full range of existing and potential adversaries, not only against worst-case scenarios, their value is undeniable.

There remains much room for improvement. U.S. efforts to defeat nuclear terrorism are insufficiently integrated across the federal government, between federal, state, and local levels, with the private sector, and internationally. This reduces the value of those detection programs that are currently underway. The Domestic Nuclear Detection Office (DNDO) has taken important steps to promote integration, but it cannot, and should not, do the entire job itself. It would be best for DNDO to focus on developing and deploying technology and on integrating radiation detection efforts, as it largely does today. Congress should explore the utility of establishing a broader system integrator in the Executive Office of the President.

An effective strategy to detect smuggled nuclear weapons would also benefit enormously from a far better understanding - a strategic intelligence assessment - of the covert nuclear threat. We are not fighting the movement of radioactive materials - we are fighting states or organizations with their own internal limits that must acquire, possibly build, transport, and detonate a weapon, all with some strategic, political, or religious goals in mind. Simply testing the sensitivity of our radiation detection instruments is thus insufficient alone for judging whether our investments are worthwhile. Without a better understanding of the enemy, we cannot adequately assess the value of our defensive investments. Congress should support a concerted effort to produce a detailed strategic intelligence assessment of the covert nuclear threat, and use this assessment as the basis for judging investments in defense against nuclear smuggling. This assessment should draw upon analysts with expertise in terrorism, rogue states, and nuclear technology, as well as on new intelligence operations as required.

You have also asked me to comment on the potential of "transformational" technology. This is technology that could lead to "dramatic improvement in national capabilities in nuclear/ radiological detection and verification." Physics imposes basic limits that must be acknowledged, but there is room for technological advance. Congress should, in principle, support long-term transformational programs, which would benefit from increased funding and from better use of the national laboratories. Congress should, however, exercise oversight to ensure that resources are deployed in ways that complement broader defensive efforts.

Outline

The remainder of this testimony is divided into five parts:

1. Describes the broad system for defending against covert nuclear attack, of which direct defense against nuclear smuggling is a part, and makes recommendations for better integrating the system.
2. Makes the case for a new strategic intelligence assessment of the covert nuclear threat, as a basis for defensive planning and evaluation.
3. Assesses the potential of transformational radiation detection technology.
4. Describes the transformational potential for detection systems that integrate radiation detection with other detection tools.
5. Explains why traditional detection efforts will be less effective against covert nuclear attack by states, and stresses the importance of attribution and deterrence in these cases.

The Defensive System

Were we able to secure all nuclear weapons and materials, there would be no need for a broader effort to prevent nuclear smuggling. Security at the source, including, most prominently, cooperative threat reduction, is the most powerful tool available, and would benefit from increased investment and attention. But it will never be sufficient alone.

A system of defensive tools, including materials and weapons security, law enforcement, intelligence, border controls, consequence management, denial of sanctuary, targeting of terrorist financing, and disruption of terrorist recruitment, can work to significantly reduce the likelihood of a successful nuclear plot, and to dissuade terrorist groups from pursuing such plots in the first place. (Preventing covert state attack is very different from preventing terrorist attack. I discuss this challenge below under "Attributing Attacks".) Even if no single defensive tool has a high probability of defeating a given terrorist attack, a combined defensive system can still be effective. If, for example, twenty independent defensive measures each have only a 10% chance of defeating a terrorist plot, they would, combined, have a 90% chance of defeating that plot. If each defensive element forces a terrorist group to alter its plot, the effect is even more powerful.

Tools for detecting nuclear smuggling must be developed and assessed in this context. That a particular defensive tool cannot defeat all terrorist plots is not reason enough for rejecting it - so long as a defensive tool complicates terrorist plots, increases their probabilities of failure, and is pursued within a broad defense, it may deserve investment.

This way of thinking about nuclear terrorism - refusing to assess defensive elements except as parts of a system - must be institutionalized. DNDO was in part an attempt to do that, but it falls short. Though DNDO includes interagency mechanisms for coordination, its efforts have been

principally focused on coordinating radiation detection programs. This is useful but insufficient, as the wide range of tools relevant to defense against nuclear terrorism, outlined above, suggests.

It is, however, natural, and perhaps inevitable, for an organization whose funds are spent primarily on radiation detection. Ultimately, DNDO should be one (major) piece within a broader effort to defeat nuclear terrorism, directed from within the Executive Office of the President. The National Counterterrorism Center (NCTC), which is responsible for strategic operational planning against terrorist threats, appears to be the right place for such coordination.

Congress should consider directing the NCTC to produce a strategic operational plan that prescribes and delineates responsibilities for defense against nuclear terrorism across the U.S. government, and to periodically assess the effectiveness of that plan. Such a scheme would help efforts to detect nuclear smuggling, and provide context for evaluating them.

Understanding the Enemy

It is meaningless to talk about the effectiveness of a defense without understanding the enemy that it faces. Yet we do not have a strong understanding of that enemy. In assessing detection of nuclear smuggling, we thus fall back against two poor substitutes. Sometimes, we adopt a narrow technical focus, evaluating technologies against quantitative goals that are at best loosely connected with careful study of terrorist plots. Here, our tendency is often to adopt goals simply because they are achievable. At the other extreme, we focus on the worst-case threat, a terrorist group that is so resourceful, flexible, and lucky that it can evade essentially any defense.

This is what many would call the "Ten-Foot Tall Terrorist". In reality, many terrorist groups have far more limited, though still very threatening, capabilities. These are the "Five-Foot Tall Terrorists". It is critical to understand these more limited threats, and to design defenses against them as well. As in military planning, defenses optimized against the worst-case threat are not necessarily the best possible defenses. Instead, defenses designed to contend with a range of enemy capabilities have the potential to be far more effective.

What does this mean in practice? The United States needs a new strategic intelligence assessment of potential covert nuclear plots. That assessment should draw upon expertise in terrorism, rogue state behavior, and nuclear technology, and outline a range of terrorist capabilities, rather than simply estimate a worst-case or most-likely threat. Novel intelligence operations can help refine this estimate - for example, intelligence operatives posing as nuclear scientists could improve our understanding of how terrorist groups might recruit technically skilled assistance. As with the strategic operational plan, this intelligence assessment most likely should be led by the NCTC. This would provide an intimate connection between underlying intelligence and strategic operational planning. It would also help institutionalize the practice of assessing the value of U.S. programs against a realistic assessment of the threats they face.

Radiation Detection: Techniques, Targets, and Transformational Potential

Materials used in nuclear weapons - uranium and plutonium - emit radiation: neutrons and gamma rays. Detectors are designed to sense that radiation. To be useful, they must be able to distinguish radiation emitted by nuclear materials from naturally occurring radiation, which may come from the earth, from building materials, from space, and from other sources. In many

cases, detectors must be able to do that in the presence of "shielding", material placed around the nuclear material that absorbs gamma rays or neutrons before they can reach a radiation detector.

Unfortunately, material used in nuclear weapons need not be highly radioactive, and hence may not emit many neutrons or gamma rays, making detection difficult. Much has been made of the difficulty of detecting highly-enriched uranium, a challenge to which I will return later. It is important, though, not to focus narrowly on this worst-case threat. Many materials that terrorists might transport as part of a nuclear plot emit considerably more radioactivity, providing greater opportunities for detection. (There is no reason to believe that terrorists can be selective, rather than opportunistic, in acquiring nuclear materials, at least without making themselves more vulnerable to defeat.) These materials include highly-enriched uranium that is below weapons-grade, that it not metallic, or that has been extracted from used nuclear fuel (as much Russian nuclear-weapons material has been). They also include plutonium, in both metallic and non-metallic forms. And stolen weapons may incorporate large masses of depleted uranium, which substantially increases radiation emissions. Detectors that can spot some but not all potential weapons or materials - an accurate description for many detectors - can be valuable.

Many challenges still remain, both in detecting low-radioactivity materials (including weaponsgrade uranium metal) and in detecting shielded materials. Here, at least four types of "transformational" technology make sense. It is too early to evaluate specific technologies, but it is useful to understand where the potential for advances exists, along with their limits.

Combined radiation detection and radiography, analyzed using new software, has the potential to substantially increase detection capabilities. Used in close proximity to a suspect source such as a cargo container (within a few meters), radiography, like an x-ray, produces an image that may be able to identify shielding material. Thus, if a terrorist group uses shielding to hide material from radiation detectors, radiography may be able to identify it. Intelligent data analysis algorithms can increase the combined value of radiation detection and radiography by automatically synthesizing data from both sources, a process that is currently labor-intensive, prone to human error, and slow. Indeed, it is this software, rather than any of the hardware used, which has the potential to be transformational, and that should be the focus of investments.

Active interrogation is also potentially transformational. Again, it must be used in fairly close proximity to a suspect source. Active interrogation bombards suspect objects with radiation. If those objects contain nuclear materials, they will, in turn, emit radiation that can be detected. In principle, such technology can be used to detect well-shielded material, so long as an intense enough radiation source is used. (Increasing the radiation source is, very crudely, like turning on a brighter light when searching for something.) However, such strong sources of radiation raise health concerns, since they can be dangerous to operators and to bystanders, among other problems. It is thus essential that development of active interrogation systems be accompanied by careful evaluation of what radiation exposure is socially acceptable, a process that has not received the same attention as the technology has. (This is a political process.) Current limits on radiation exposure may already be too low. Moreover, in a very high threat environment - for example, in the aftermath of a theft of nuclear material - society will likely be willing to accept much more hazardous means of inspecting cargo. Yet if we do not develop technologies in advance, we will not be able to exploit such situations. Ultimately, though, safety issues will

place limits on the potential of active interrogation.
Detectors that are more efficient and that have better energy resolution than current models might also be transformational. (Their potential, however, is more limited than that of active interrogation, though they do not carry the same dangers.) What does this mean?

Radiation detectors only detect a fraction of the radiation emitted by nuclear materials. That fraction is called their "efficiency". While we cannot change the fact that many nuclear materials emit little radiation - these are the "limits of physics" that many refer to - we can improve how much of that radiation we detect, allowing us to better find nuclear materials.

Radiation detectors are also characterized by their "resolution". Radiation varies in energy, and the energy of radiation can sometimes be used to distinguish nuclear material. If a detector can more effectively discriminate between different energies - if it has improved "resolution" - it will be better at identifying nuclear material. Think of energy as color, and the gamma rays emitted by a particular type of nuclear material as "red". A detector with poor energy-resolution is color-blind - it cannot use color to spot the nuclear material. Improving detector resolution is like improving ability to see in color, and thus to identify nuclear material.

A final potential for transformational radiation detection technology lies in integrating data from large numbers of detectors. This has both hardware and software components. It requires reduction in weight, cost, and power requirements for detection systems, so that large numbers can be deployed cost-effectively, and often in mobile configurations. It requires software to dynamically integrate data from a large number of detectors. One example of such a program might involve radiation detectors mounted on large numbers of police cars, transmitting data to a central location where it is continuously combined. Advances in computational power would also help advance these technologies.

These technological innovations might also be combined. For example, higher efficiency radiation detectors might be combined with radiography using advanced data analysis.
How should this affect American investments? In FY06, DNDO received $56.6 million for "Transformational Research and Development". In contrast, only one major program area at DARPA, which supports transformational research through the Department of Defense, was funded at less than $100 million during FY06. As DAPRA understands, ambitious, high-risk research requires funding many failures in order to yield a single success. Transformational efforts would profit from expanded funding.

Congress should consider earmarking such funds for the national laboratories, which are currently excluded from applying for several critical DNDO transformational R&D grants. (They may apply as subcontractors.) This occurs despite their having deep strength in relevant technologies. Moreover, if we are to direct efforts at detecting realistic nuclear weapons, rather than just generic samples of radioactive materials, we must exploit the understanding of weapons design that the laboratories have accumulated over more than half a century. DNDO has asserted that most of its transformational work will be unclassified; as a result, it will not be able to exploit this opportunity. The national laboratories will.

In the long term, transformational detection efforts should be assessed against a new, nuanced strategic intelligence assessment, and within the context of a broad strategic operational plan.

Integrating Radiation Detection into a Broader System for Detecting Nuclear Smuggling
Radiation detection is not the only way to spot nuclear smuggling, especially if terrorists decide to smuggle an assembled bomb. In many cases, explosives detection may play an important role, as might detection of the weight and bulk of a weapon or of nuclear materials.

Automated systems that integrate data from multiple detectors would be particularly valuable. Strategists should also explore automated means for integrating radiation detection with non-technical detection. For example, it would be useful to develop algorithms for airports and official border crossings that combine radiation data with passenger profile information to yield combined assessments of nuclear threats. A similar scheme could be useful for identifying suspect cargo containers, based on radiation detection and non-technical intelligence.

In many cases, radiation detection will play a supporting, rather than a leading, role. This is particularly notable in defending against nuclear smuggling at non-official points of entry, such as land, sea, and air borders. Transformational schemes envisioning continuous and universal radiation monitoring of American borders are unrealistic. Instead, efforts aimed at identifying and interdicting terrorists attempting to enter the United States, regardless of whether they are involved in nuclear plots, will play the leading role, with radiation detection supporting them.

Consider, for example, attempts to smuggle nuclear weapons or materials across the southern border. The probability of an illegal immigrant successfully crossing the border after one attempt is likely less than fifty percent; such low odds of success might well deter a would-be nuclear terrorist from attempting a crossing. What makes illegal immigration easier is the "catch-and release" policy that affords would-be-immigrants multiple chances to attempt illegal entry.

Portable radiation detection equipment can, however, be used to ensure that individuals caught at the border while carrying nuclear weapons or materials are not released. Here, radiation detection plays a critical but supporting role. Similar schemes might be applied to aircraft intercepted while illegally entering U.S. airspace. Applying this approach on the water presents greater challenges, as the United States currently has much weaker capabilities to detect illegal sea-based entry. Addressing this requires efforts to improve maritime domain awareness, and maritime interdiction capabilities, rather than to improve radiation detection. This emphasizes the need for a broad defensive plan, and cautions that technical detection investments must not outpace other complementary, non-technical, homeland security needs.

Intelligence can also multiply the effectiveness of radiation detection. If we know or strongly suspect that terrorists have acquired nuclear weapons or significant amounts of nuclear materials, a surged response is possible. Such detection begins at the source of nuclear materials and weapons. For over a decade, the United States has been helping other countries install systems for protecting their nuclear weapons and materials (so-called MPC&A systems). If terrorists acquire materials or weapons, MPC&A systems will in many cases provide warning, allowing a surged response to any ensuing attempt at nuclear smuggling. The United States should attempt to secure agreements with facilities that receive MPC&A assistance, requiring that they promptly share warning information. DNDO is already tackling this challenge, and should be strongly supported by other parts of the U.S. government. It would be wise to go beyond this and develop protocols and agreements for sharing warnings of theft, including from facilities secured without U.S. assistance.

Such warning may be the most powerful source of intelligence that can be leveraged by detection systems. Its value would be strengthened if the United States stockpiled equipment needed for a surged response, which could be deployed only when necessary. (Despite the high prices of many detection systems, the bulk of their costs come from the labor required to operate them.)

Other sources of intelligence should also be pursued. For example, if terrorists are caught attempting to bribe radiation detector operators, intensified interdiction efforts might be mounted. Advance development and stockpiling of detection equipment would be essential.

Attributing Attacks

Against states, which generally have deeper resources and more extensive military and intelligence capabilities than terrorist groups, American efforts to directly defeat nuclear smuggling are far less likely to be successful. In particular, states will have greater abilities than terrorists will to evade radiation detection and border control efforts. Our best hope against these threats is to enhance deterrence by improving our ability to attribute covert attacks to their sponsors, thus allowing us to threaten retaliation. (This is a form of detection, albeit post-attack detection.) Attribution would work through a mixture of traditional forensics and technical tools that exploit nuclear-specific signatures. The latter would operate primarily by analyzing samples of material dispersed in a nuclear attack, and comparing them to a database of "fingerprints" for various nuclear states. Our greatest current deficiency on this front is in the fingerprint database. Theoretical analyses of material produced by suspect facilities, along with intelligence operations to obtain foreign material samples, would be valuable. So would better coordination: multiple government agencies with strong capabilities in this area, such as the CIA and the DOE, are not fully sharing what they know with each other.

International cooperation, done with appropriate consideration for secrecy, would also help enhance deterrence.

Summary

Six points should be kept in mind when thinking about detecting smuggled weapons:
1. Securing nuclear weapons and materials at the source will always be the most powerful defensive tool.
2. Within the context of a broader defensive system, efforts to detect nuclear smuggling can be valuable.
3. It is essential to assess these efforts against a wide range of realistic threats, not only against semi-arbitrary numerical targets or worst-case scenarios.
4. Transformational technology has real potential but firm limits. It is as much about innovative software, concepts of operations, and leveraging intelligence, as it is about hardware.
5. Technology will often play a supporting role to traditional tools for controlling land, sea, and air borders. Those traditional tools must receive strong support.
6. Detection and interdiction are much weaker tools against covert state threats than against terrorist plots. Against state threats, enhancing attribution capabilities is critical.