NUCLEAR DEFENSE WORKING GROUP ROUNDTABLE

Surge, Net Assessment, and Intelligence in Setting National Nuclear Terrorism Policy

December 6, 2005

The Center for the Study of the Presidency convened the *Nuclear Defense Working Group on Surge and Net Assessment* under the chairmanship of Dr. Richard Wagner to attend to critical issues in developing, deploying, and managing a more comprehensive defense against the smuggled nuclear threat.

The Working Group met during the final stages of a senior-level task force charged with developing a layered defense against weapons of mass effect, which was commissioned by the Secretary of Homeland Security's Advisory Council and will report to Secretary Chertoff in January 2006.

The Working Group, which included participants with senior White House, Defense Department, Homeland Security, and Intelligence Community experience, discussed definitions of success with emphasis on *preventing* covert attack with a nuclear weapon and offered a specific focus on how the U.S. Government should think about intelligence in this effort. The roundtable discussion also highlighted the use of red teaming and net assessment. The following represents a distillation of the themes and observations that emerged during the December 6 seminar. All comments were off the record.

~*Highlights*~

I. Define a Theory of Success

The White House must define a theory of success in defending against the smuggled nuclear threat. The Administration has issued a strategy for combating terrorism and a strategy for combating WMD. However, there remains the need to create a strategy to combat the threat residing at the intersection of these two issues: WMD terrorism.

The job of preventing a successful attack of this kind is so daunting that policy must consider the importance of first countering the tendency to view defense as hopeless and focus only on preventing access to nuclear material (important as that is). Furthermore, making all the layers of defense work together and bridging the various concepts of success will require an extraordinary degree of common understanding across departments and agencies.

1020 19th Street, N.W., Suite 250 • Washington, DC 20036 • Tel. 202-872-9800• FAX 202-872-9811
www.thePresidency.org

Absent a czar in this area, it is imperative to have a common and deep understanding of how we will succeed. Initially, this entails defining success factors that can together form the basis for a comprehensive strategy to combat the smuggled nuclear threat. Those factors include:

1. Securing nuclear material and weapons available from vulnerable military, civilian, and commercial sources/sites;
2. Declaratory and de facto deterrence policy that is comprehensive and robust;
3. Intelligence about the nature and trajectory of the threat;
4. Detection capabilities deployed globally and as part of a layered architecture;
5. Counterterrorism operations ranging from psychological operations to use of force;
6. Interdiction;
7. Consequence management; and
8. Attribution.

The Administration has recognized these as the foundation for a smuggled nuclear defense, but has added the importance of de-legitimizing radical extremism that seeks to obtain and use WMD for attack or for blackmail. A critical component to overall success, however, is consistent attention, visibility, and funding.

II. Identify the Threat Spectrum

The smuggled nuclear threat presented by terrorist organizations seeking to pursue al Qaeda-style objectives against the United States should be considered as a possibility – albeit certainly a likely one – along a spectrum of potential perpetrators seeking to attack the U.S. with a nuclear weapon. At the other end of that spectrum is nuclear attack by a state (or a loose entente between states) using the methods of terrorists (i.e. covert delivery, civilian targets), but with the objectives of states. A national policy for nuclear defense must also consider a "hybrid" operation as equally likely. A hybrid threat would include terrorists and states making common cause in any of a possibly wide variety of relationships and operational arrangements, and for any of a wide variety of reasons. Certain hybrids might not have been encountered before, and thus we might be surprised by both objective as well as method.

1020 19th Street, N.W., Suite 250 • Washington, DC 20036 • Tel. 202-872-9800• FAX 202-872-9811
www.thePresidency.org

Along with general defensive and offensive measures, our deterrence policy should evolve to counter the hybrid scenario, which presents a challenge much different from the conventional Cold War balance that relied upon a level of certainty in attribution and corresponding threat of overwhelming retaliation. To the extent that states are complicit, retaliation-based deterrence could be strengthened by improving capabilities for attribution.

III. Adapt Deterrence

Deterrence in the context of terrorists deploying a nuclear weapon also must adapt from Cold War models of retaliation. When potential perpetrators such as these care little about retaliation for various reasons, deterrence must seek to exploit a fear of failure. Programs must be designed and arrayed to manage a layered defense that complicates an adversary's efforts in several ways. The net result should be either of two outcomes:

- First, a layered defense will force an adversary to consider the likelihood of success too low for him to risk losing an asset as valuable as a nuclear weapon or special nuclear material. Highly selective and highly sensitive sensor capabilities serve a significant role in accomplishing this, but other measures, such as psychological operations, contribute greatly to forcing the adversary to reconsider whether to deploy. This type of deterrence could be reinforced by ensuring the adversary knows a lot about some of our detection capabilities but also by deliberately creating uncertainty in the attacker's mind that he will be able to know enough about our defenses to be able to design a successful attack.

- The second aspect of this type of deterrence forces an adversary to complicate his operations enough (i.e. involving more accomplices, more money, etc) that his likelihood of interdiction increases without him aborting the operation before disruption and, ideally, capture.

The resilience or ability to mitigate the impacts of a WMD attack can contribute to a deterrence strategy. Deterrence in general could be reinforced by combining, in one coherent operational and doctrinal whole, these four competencies: surge, consequence management, attribution, and retaliation. Therefore, when assessing the deterrent values of various countermeasures, consequence management can be considered together with forensics/attribution and retaliation.

1020 19th Street, N.W., Suite 250 • Washington, DC 20036 • Tel. 202-872-9800• FAX 202-872-9811
www.thePresidency.org

IV. Expand WMD Intelligence Demand/Consumption

Improving the defense against smuggled nuclear weapons includes both a greater commitment to securing loose nuclear material and developing/deploying better "close-in" monitoring of targets. The Secretary's WME Task Force can help draw attention to the former and the DNDO certainly promises to make progress in generating the latter. A less understood requirement today, however, concerns developing a better "demand articulation" of WMD intelligence, specifically with regard to the smuggled nuclear threat. For example, CIA's WINPAC has traditionally found itself relied upon by the State Department more than any other intelligence customer because such intelligence was used primarily for enforcing sanctions and shaping diplomatic demarches on proliferation issues.

Today, the WMD intelligence consumer should be defined by a wider constellation of authorities, to include the Departments of Homeland Security and even Health and Human Services. However, these "post-9/11 customers" need to be trained to be smart consumers, to ask the right questions, and to understand the answers (DoD could help train them for this). Their leadership must actively task intelligence community organizations such as the National Counterproliferation Center and the National Counterterrorism Center. For example, the Domestic Nuclear Detection Office is responsible for creating a deployment strategy, or "global architecture," to operate across all layers in defending against smuggled nuclear weapons and material. To do so, the DNDO must consider intelligence about the trajectory of the current nuclear threat, including potential perpetrators, means of delivery, and likely sources of illicit nuclear material. Finally, the White House needs to tell the Intelligence Community to greatly cater to these "post-9/11 customers."

Establishing a clearer link between intelligence analysis and action will help the process of modernizing the intelligence cycle and corresponding bureaucracy, such as the NCPC and NCTC. The CIA underwent a similar transformation when its Counterterrorism Center developed from a place where scholars studied terrorism into an outfit where experts fought terrorism. This change was driven in part by a new customer base at DOD that placed counterterrorism into the intelligence consumption cycle. DHS must – perhaps through DNDO – do the same with NCPC and NCTC, but so also must other parts of the homeland security leadership at HHS, DOE, and elsewhere.

WME threat intelligence may benefit from a measured shift away from evidence-based analysis. Modeling can provide understanding beyond the

1020 19th Street, N.W., Suite 250 • Washington, DC 20036 • Tel. 202-872-9800• FAX 202-872-9811
www.thePresidency.org

currently available set of knowns that should inform a nuclear defense strategy. However, that one can model almost anything risks diluting the value of this type of analysis. Therefore, a methodology should be developed that can bound intelligence modeling on the WME threat.

V. Institutionalize Net Assessment for the Smuggled Nuclear Threat

Action-oriented agencies, however, tend not to think very far into the future. If both NCTC and NCPC become action agencies, then another institution *must* look to the future. Institutionalizing "net assessment" is a way of doing so. Net assessment:

- Transcends current intelligence;
- Looks into the farther future – at least two cycles of action/reaction;
- Takes the very broad geopolitical context into account;
- Considers how we and adversaries might shape the environment; and
- Always takes into account the adversary's point of view and his possible adaptations to our strategies (and thus both uses and stimulates red-teaming and red-blue exercises).

How net assessment should be institutionalized remains unanswered. The Intelligence Community should not house an overall net assessment effort since it needs to reach beyond current intelligence and evidence. Whether it should be located at DHS is unclear, too, but because the assets, authorities, and responsibilities to combat the smuggled nuclear threat reach above and beyond the Department.

In DOD experience, Net Assessment's relationship to intelligence has been controversial. Because of this, and to preserve its focus on the farthest future, certain practices have proven prudent. Net assessment should not be used to support budgets. Even using net assessment to build policy should be done sparingly. Rather, it should be employed only to shape the thinking of policy-makers. Net assessment should make use of "path gaming" and should spend as much time as needed to find the small handful of the very best thinkers.

VI. Institutionalize Red/Blue Exercises for the Smuggled Nuclear Threat

Exercises, red-teaming, and gaming serve a valuable role for the military and could benefit the national effort to combat the smuggled nuclear threat by dealing with each of the success factors listed above (Paragraph I). Eventually, red/blue exercises could be done on a large scale of 1000 people or more. A

comprehensive regimen of exercises and red-teaming would be useful for at least four reasons:

1. The visibility that the U.S. is doing something to counter this threat has an implicit deterrent value. Exercises should be structured with this in mind.
2. We need the practice: Red-teaming and gaming have the concomitant benefit of familiarizing stakeholders at the operational level with each other, to build trust among them, to form crucial back-channel communications, and to shape and share best practices.
3. Exercises can institutionalize "red/blue thinking."
4. Red-teaming can help develop metrics to gauge capability, which are especially needed to flesh out a Theory of Success.

VII. Resolve or Manage Institutional "Tensions"

Tensions exist between interests, authorities, and bureaucracies related to a layered defense against the smuggled nuclear threat. A national policy will identify some of these and offer ways they can be managed, balanced, and, where useful, created. Related tensions include:

1. An emphasis on prevention versus reaction (DNDO)
2. immediate improvements (COTS) versus long-term progress (transformational)
3. evidence-based intelligence versus analysis modeled on the possible
4. The role of DOD in executing its own operational responsibilities vs. a much broader role for DoD that brings its competencies in planning large operations and in advancing R&D into effective fielded capabilities to other agencies involved in the layered strategy.

Another tension exists between "homeland security" and "national security." Beyond the need for an intellectual reconciliation between the two, White House leadership on this issue remains incomplete. The White House Homeland Security Council staff is approximately one quarter the size of the National Security Council. More importantly, HSC staff leadership do not have the same rank and authority as their NSC counterparts.

Solutions to this challenge also require examining the relationship between the HSC and NSC and whether some issues nominally on the HSC side should thus be shared in some way with the NSC because the latter has more staff and

1020 19th Street, N.W., Suite 250 • Washington, DC 20036 • Tel. 202-872-9800• FAX 202-872-9811
www.thePresidency.org

clout. This may be especially true for clandestine attack with WMD, which could be carried out by states, and is more like national defense than homeland security. Ultimately, the President defines these two Councils by how he uses them.

VIII. Develop Surge Techniques and Capabilities

As we deploy better defenses, we could expect to have better tactical warning (perhaps of weeks or even months). With credible warning that an actual attack was in its operational phase, we might want to exercise certain options we would not find practical or productive absent such warning. This is even truer after a first successful or even failed attack. Options might include: spending a lot more money a lot more quickly on R&D, cutting red tape to accelerate acquisitions, using the military much more extensively, conducting forward operations against the threat, and disrupting commerce and travel.

To exercise these options, some prerequisites would have to be in place to include special authorities, pre-positioned equipment, signed contracts to surge production of equipment, MOUs with allies and the private sector.

1020 19th Street, N.W., Suite 250 • Washington, DC 20036 • Tel. 202-872-9800• FAX 202-872-9811
www.thePresidency.org