The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND
- Browse Books & Publications
- Make a charitable contribution

For More Information
- Visit RAND at www.rand.org
- Explore RAND Testimony
- View document details

Limited Electronic Distribution Rights
This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.
Developing Robust Border Security Technologies to Protect Against Diverse and Adaptive Threats

Addendum

BRIAN A. JACKSON

CT-294/1

December 2007

Document submitted on December 17, 2007 as an addendum to testimony before the House Science and Technology Committee, Subcommittee on Technology and Innovation on November 15, 2007
Brian A. Jackson
The RAND Corporation

Developing Robust Border Security Technologies to Protect Against Diverse and
Adaptive Threats
Addendum

Submitted to the Committee on Science and Technology
Subcommittee on Technology and Innovation
United States House of Representatives

December 17, 2007

The subsequent questions and answers found in this document were received from the Committee for additional information following the hearing on November 15, 2007 and were submitted for the record.

Questions Submitted by Subcommittee Chairman David Wu

Question 1. In your testimony, you said, "the effectiveness of security technologies can degrade as our adversaries adapt and alter their behavior in response to the introduction of defensive measures. That adaptive behavior can pose a significant risk to the security benefits new defensive technologies are intended to provide and, therefore, must be considered in technology planning." In your opinion, does DHS S&T recognize the need for adaptive, flexible technology planning? How do the contributions of various advisory groups, such as Integrated Product Teams and the HSSTAC affect DHS S&T's ability to adapt to new challenges?

Answer 1. Our research on the effects of terrorist adaptive behaviors on the efficacy of defensive measures was sponsored by DHS S&T's Office of Comparative Studies to identify the implications for S&T planning for combating terrorism. Because RAND has not had the opportunity to examine DHS S&T's technology planning processes or the activities of groups like the Integrated Product Teams and the HSSTAC, I unfortunately cannot provide an informed answer on the extent the ideas developed in our or others' work on this topic are reflected in DHS planning efforts.

Question 2. You specifically mention how adversaries have been able to defeat the technologies identified as priorities in the bill: unmanned aerial vehicles (UAVs), tunnel detectors, and anti-
counterfeit technology. How should these identified vulnerabilities affect how DHS proceeds in these research areas?

**Answer 2.** Terrorist groups’ past efforts to degrade the effectiveness of priority technologies like UAVs, tunnel detectors, and anti-counterfeiting technologies can inform research planning in two ways.

First, the ways that terrorist groups have found to do so provide lessons for improving future technologies that can be directly applied in current research activities. If approaches can be devised that render terrorists’ past counter-technology strategies ineffective, our future defenses will be stronger as a result. Our research has shown that responding to terrorist adaptive behavior can involve modifications to the technical systems themselves, which would need to be an integral part of R&D programs, but frequently require changing the concepts of operation for how technologies are used as well. This emphasizes that in developing new defensive measures it is important to consider the ways those technologies will be used as part of the development process, since those concepts of operation may be critical to maintaining the technologies’ effectiveness. It also underscores the importance of the transition efforts to move new technologies to end users and help shape their application.

Second, in designing research programs for these priority technologies, the principles identified in our research and summarized in my testimony are important to ensure that the defensive measures we develop in these areas are robust to adversary adaptive efforts. Including testing, red teaming, and small scale technology pilot efforts in R&D programs is needed to identify and address vulnerabilities to their effectiveness. Furthermore, given that adversary groups have shown remarkable flexibility to respond to even sophisticated technologies, it is also critical to maintain reasonable flexibility in the technologies being developed and to build R&D portfolios in each of these areas (i.e., rather than focusing on only a single technology choice) to preserve “fall back” defensive options if the effectiveness of deployed technologies is compromised.

**Questions Submitted by Full Committee Ranking Member Ralph Hall**

**Question 3.** What assessment technique would you suggest for determining the funding priorities among threats such as border security or radiological detection?

**Answer 3.** In RAND’s past research and testimony on homeland security, we have advocated that funding priorities should be informed by risk analysis – an assessment of the threat of specific attacks, the vulnerability of targets of concern to those attack modes, and the consequences that would occur if an attack was successful. Use of risk analysis in policy planning ensures that
priorities are defined not just by one these three factors in isolation but by all three together, providing a way of considering high probably, lower consequence events – such as “everyday” illegal border crossings by individuals – with lower probability but potentially higher consequence events – such as radiological material being smuggled into the country.

A risk-informed priority setting process for R&D would consider the seriousness of individual risks and select technology priorities and options based on their ability to reduce those risks. The results of our research on terrorist responses to defensive measures could contribute to such a process since those responses degrade the effectiveness of defensive technologies, thereby cutting their ability to reduce risk.

**Question 4. What implications does your research have for the appropriate balance between short-term and long-term research projects? Are incremental changes to technological defenses enough to stay ahead of opponents' counter-efforts?**

**Answer 4.** It is difficult to provide a general answer to whether incremental, short-term technological changes are enough to stay ahead of adversary adaptive efforts. For some technologies, incremental efforts may make it possible to maintain a defense’s efficacy for some time, though it is unlikely to do so forever. In other cases, depending in large part on the specific way the opponent has found to defeat the technology, incremental changes may provide little benefit. For example, if an adversary has found a way to avoid the functioning of the technology entirely (one of the four strategies our work identified that were highlighted in my testimony), incremental change is unlikely to be enough. The importance of both short-term and long-term research projects is therefore a part of the “portfolio approach” to developing defenses our work suggested, where it is longer term work that may be the source of the “fall back” defensive options if today’s technologies are breached. Focusing disproportionately on shorter term efforts risks creating a defense that cannot respond to future changes in the threat.

While it is easy to say that both short- and long-term focused work are needed, the resources available for supporting research and development are not infinite and resource constraints must limit the number and scale of activities that can be pursued simultaneously. As a result, in thinking about portfolios of defenses we are not suggesting that multiple “full scale” technology programs be pursued at once. Instead, what is needed is portfolios of smaller scale research, pilot, and technology evaluation efforts that maintain a group of options at differing levels of maturity that be then called on – and scaled up – if and when they are needed.