TESTIMONY

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

BRIAN A. JACKSON

CT-294

November 2007

Testimony presented before the House Science and Technology Committee, Subcommittee on Technology and Innovation on November 15, 2007

Published 2007 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Brian A. Jackson[1]
The RAND Corporation

Developing Robust Border Security Technologies to Protect Against Diverse and Adaptive Threats[2]

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

November 15, 2007

Chairman and distinguished Members: Thank you for inviting me to speak on the issue of border security technology as the House Science and Technology Committee begins the process of considering legislation focused on developing the next generation of border and maritime security technologies. I was asked to provide testimony about a recently completed RAND research effort for the U.S. Department of Homeland Security, Science and Technology Directorate, Office of Comparative Studies, focusing on the role of technology in homeland security activities.[3]

As part of homeland security efforts, technology systems play a key role within a larger, integrated strategy to counter the efforts of violent and criminal organizations and to protect the public. Information and detection technologies gather data on individuals, vehicles, and behaviors; are used to monitor sites and areas of concern (including border information systems aimed at identifying individuals who should be not allowed to enter the country); help detect concealed weapons or contraband; and manage collected information so such information can be drawn on later to guide security decisions. Technologies such as barriers and setbacks harden targets or

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. The series records testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. 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. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/294/.

[3] The results of this research effort have been published in a series of RAND reports focusing on the use of technology by terrorist groups and security organizations combating terrorism:

Breaching the Fortress Wall: Understanding Efforts to Overcome Defensive Technologies, Brian A. Jackson et al., RAND MG-481-DHS, 2007, available at http://www.rand.org/pubs/monographs/MG481/

Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies, Kim Cragin et al., RAND MG-485-DHS, 2007, available at http://www.rand.org/pubs/monographs/MG485/

Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons, James Bonomo et al., RAND MG-510-DHS, 2007, available at http://www.rand.org/pubs/monographs/MG510/

Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations, Bruce W. Don et al., RAND TR-454-DHS, 2007, available at http://www.rand.org/pubs/technical_reports/TR454/

Freedom and Information: Assessing Publicly Available Data Regarding U.S. Transportation Infrastructure Security, Eric Landree, et al., RAND TR-360-DHS, 2007, available at http://www.rand.org/pubs/technical_reports/TR360/

deny individuals access to the areas they want to enter or attack. Technologies such as communication systems coordinate response activities to increase the chances that terrorist or other illegal activities can be interdicted and stopped.

Our work has examined security technologies in the context of long-term conflicts between law enforcement and security organizations and terrorist groups. Much of this research focused on how the effectiveness of security technologies can degrade as our adversaries adapt and alter their behavior in response to the introduction of defensive measures.[4] 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. The testimony provided today is drawn from this research and focuses on the parts of the study that specifically address technologies relevant to border security.[5]

Although preventing a terrorist attack is one reason for the security measures at our nation's borders, it is not the only goal those measures are intended to achieve.[6] It is estimated that several hundred thousand individuals enter the United States illegally each year.[7] Most people seeking to cross the U.S. border illegally are not doing so to conduct terrorist activities. Rather, they are seeking to enter the country themselves, smuggle drugs, move other illicit goods, or engage in human trafficking. The shipping of illicit cargo through legitimate means—e.g., through the container shipping system—is also a concern. Although such individuals and groups are not motivated by the same factors as terrorist groups, they are nonetheless similarly determined to succeed and will respond to defensive measures placed in their path to hinder them. As a result, the broader lessons we identified about designing technologies that are robust to terrorist group adaptation are similarly relevant to the other challenges and threats that border protections are designed to address.

The core message of my testimony today is that in our technology planning and development we must explicitly consider the risk to the performance of our border security technologies that is posed by the competitive, action-reaction dynamic that exists between our security efforts and the

[4] *See Breaching the Fortress Wall: Understanding Efforts to Overcome Defensive Technologies*, Brian A. Jackson, *et al.*, RAND MG-481-DHS, 2007, available at http://www.rand.org/pubs/monographs/MG481/

[5] While these remarks draw both on my work and that of my co-authors and colleagues, the specific content of my testimony is my responsibility alone. Additional information on RAND's research relevant to border security challenges is included in Michael A. Wermuth and K. Jack Riley, "The Strategic Challenge of Border Security," Testimony before the Committee on Homeland Security, Subcommittee on Border, Maritime and Global Counterterrorism, U.S. House of Representatives, March 8, 2007, available at http://www.rand.org/pubs/testimonies/CT275/

[6] U.S. Customs and Border Protection, Office of Border Patrol, "National Border Patrol Strategy," undated.

[7] See, for example, estimates in Government Accountability Office, "Illegal Immigration: Border-Crossing Deaths Have Doubled Since 1995; Border Patrol's Efforts to Prevent Deaths Have Not Been Fully Evaluated," GAO-06-770, August 2006.

adversaries they target; if we do not do so, we risk spending resources on defenses that ultimately will not deliver the protection we expect. To do so we must

- include testing, red-teaming, and experimentation in technology development efforts to ensure new security measures are robust to adversary adaptation
- maintain flexibility in our security technologies to the extent possible so we can respond to changes in the behavior of our adversaries that degrade or eliminate the protection the systems provide
- ensure *defense in depth* by developing portfolios of defensive measures that provide "fall back" options if adversaries learn how to avoid our primary defensive systems

Finally, although the focus of today's hearing is on developing technology, we must also remember that security is ensured not by technical systems alone but also by the organizations and people who use them and the concepts of operation that guide how they are used.[8] How we use technologies is a key determiner of how vulnerable or robust technologies are to our adversaries' adaptive efforts and helps to determine the net security effect of adversaries' efforts to break through our defenses. As a result, how technologies will be used in border security efforts should be considered during technology planning and research roadmapping to make sure we capture the full set of factors that will define their future security performance.

How Can The Responses of Terrorist Groups or Other Adversaries Affect the Protective Value of Security Technologies?

New security technologies are frequently costly, making it imperative that we ensure, to the extent possible, that they will produce enough benefits in improved security to justify the investments required to develop and deploy them. If there is a substantial risk that the security benefits of a particular technology will not be realized, that risk could make an otherwise promising technology a poor choice.

In our research, we examined one such risk: How changes in behavior by terrorist groups could reduce or even eliminate the protective value of technological security measures. To identify how technologies were vulnerable to terrorist group adaptation, we looked at how a number of such organizations responded when they were challenged by new defensive measures. Because we

[8] See, for example, David Aguilar, Office of Border Patrol, "Border Security: Infrastructure, Technology and the Human Element," Testimony Before the Subcommittee on Border, Maritime and Global Counterterrorism, Committee on Homeland Security, U.S. House of Representatives, February 13, 2007; RADM David P. Pekoske, U.S. Coast Guard, "Border Security: Infrastructure, Technology and the Human Element," Testimony Before the Subcommittee on Border, Maritime and Global Counterterrorism, Committee on Homeland Security, U.S. House of Representatives, February 13, 2007; and Jay Cohen and Gregory Giddens, Department of Homeland Security, "How Can Technologies Help Secure Our Borders?" Testimony Before the Committee on Science, U.S. House of Representatives, September 13, 2006.

were interested in lessons relevant to today's homeland security context, we examined four comparatively sophisticated terrorist groups that were in conflict with sophisticated states:

- Palestinian terrorist groups in Israel
- Jemaah Islamiyah (JI) and affiliated groups in Southeast Asia
- Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka
- Provisional Irish Republican Army (PIRA) in the United Kingdom

We found that the groups responded to security measures put in place by states or across regions with a set of four countertechnology strategies to limit the effect of the defenses on their operations. Specifically, they *changed their operational practices in ways that made the defenses less effective, used new technologies of their own to counter them, moved to avoid the defensive measures, and attacked the security technologies directly*. U.S. experience with individuals and organizations seeking to cross our border illegally shows these same broad strategies are relevant to help design current efforts to secure the country and to develop the technological tools needed to do so.

To illustrate the effect that groups changing their behavior has on the effectiveness of defensive measures, I discuss here a few of the ways the terrorist groups we studied reduced the effectiveness of protective technologies, circumvented the technologies entirely, and even attacked or corrupted the defensive measures that were getting in their way.

In many cases, terrorist groups found ways to change their behavior to render protective measures less effective. For example, the majority of the four terrorist groups responded to weapons-detection technologies by breaking down their weapons materials into small quantities (such as smuggling explosives in toothpaste tubes or cookie tins) or otherwise shielding them from detection technologies to enable smuggling or attack operations. The various ways they did this included shipping explosives obscured by strong-smelling spices or hiding them in noxious cargos like rotting fish to conceal their odor from dogs or confuse other detectors.

PIRA spent considerable time conducting "challenge-response" studies to determine the limitations of surveillance systems in an effort to learn what the systems could and could not detect and to assess the areas they covered. The group then used that knowledge to operate in ways and at times that were less likely to be detected. For example, armed with the knowledge that specific weather and lighting conditions made some sensors less effective, PIRA planned its movements and operations accordingly.

The strategies we discovered in our case studies are similarly relevant to the nation's border security challenges. For example, in 2004 testimony before the House Select Committee on

Homeland Security, Lawrence Wein of Stanford University raised questions about whether terrorist groups could render the fingerprint biometric scanning done by the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program less effective by selecting operatives whose fingerprints either will not scan well or have been deliberately altered to defeat the scanning.[9] It is also well known that smugglers seeking to bring illegal narcotics and other materiel into the country frequently alter their operational practices to conceal their cargos from search-and-detection approaches.

When they could do so, terrorist groups avoided defensive measures entirely, neutralizing their protective benefits. To avoid identification requirements and databases used to flag known or suspected operatives, most groups relied on false documents and identification credentials to hide the true history and identity of both people and vehicles. Some groups even took this strategy to the extreme, coercing innocent people with no connection to terrorism—by threatening their lives or the lives of their loved ones—to transport people or weapons through checkpoints with identity checks.

Avoidance can work for surveillance systems as well: As part of Israeli security measures, overhead surveillance with unmanned aerial vehicles (UAVs) or helicopters were used to monitor areas near the border where attacks were staged. In rural areas, Palestinian groups used spotters on rooftops in the West Bank or Gaza Strip to watch for the vehicles and warn militants to stay out of sight when the surveillance systems were in the area.

To avoid some defenses, groups had to make more drastic changes. In response to significantly strengthened border security at ports of entry in the nations where it operated, JI shifted its operations from seeking to move people and material through defended areas like airports to less monitored and defended maritime or land borders. In response to the security barrier erected around Israel, Palestinian groups reportedly deployed specially crafted ladders that enabled them to climb over the security fences without triggering the sensors at the top. In addition, the groups have also engaged in extensive tunneling to circumvent the barrier around Israel and border security between Egypt and Gaza, enabling weapons smuggling and infiltration. The Israeli Defense Force (IDF) notes that Palestinians have taken a number of measures to avoid having their tunneling operations detected, including building tunnels in residential areas (entrances are often through private homes and property), digging at night, transporting displaced dirt and sand out of the vicinity of the tunnels, and staging diversionary strikes against IDF outposts to conceal the sound of explosives.

[9] Lawrence M. Wein, "Disrupting Terrorist Travel: Safeguarding America's Borders Through Information Sharing," Testimony before the U.S. House of Representatives, Select Committee on Homeland Security, September 30, 2004.

At our own border, individuals seeking to enter the United States illegally have responded to the deployment of border fencing in similar ways, for example by altering their routes and seeking to enter the country at more remote, unfenced locations. Drug smugglers have similarly shifted their routes and transport modes to avoid interdiction efforts.[10] Tunneling under the barriers has also been observed.[11]

Finally, in some limited cases, terrorist groups simply attacked the defensive measures hindering their activities. In response to the extensive use of information systems in the counterterrorism effort against PIRA, the group sought to attack information systems directly to corrupt or steal information (at one point breaking into a police facility to steal files). The group also used information-gathering technologies such as the security organizations' own public tip line to inject false information into the system. The group also used hoax operations and triggered detection technologies to cause false alarms as ways to stress the capabilities of the security and response forces. In some cases, the groups we studied directly broke down barriers and defenses that got in their way, either by using larger bombs or by staging more complex operations to neutralize the defense before a larger attack took place. In response to the construction of fencing on the U.S. land border, similar efforts to damage or breach the barrier have been observed.[12]

How important were terrorist efforts to "learn their way around" defensive measures? For most defensive measures, the groups could find ways to reduce their effectiveness and degrade their protective value. However, in some cases, terrorist groups paid a substantial price to neutralize a defense; for example, although a tunnel might make it possible to get under a security barrier, the effort the group had to spend to construct it was effort that could not be devoted to violent activities. When this was the case, even if the technology did not necessarily deliver the full protection it was expected to—or deliver it in the way that was expected when it was designed—its value could still be considerable.

Then again, in other cases, the cost to the group to evade a defensive measure was relatively small; in one particularly dramatic case cited by a counterterrorism professional we interviewed, PIRA learned that a sophisticated surveillance system incorporating facial recognition technology could, under the right circumstances, be countered by simply wearing a baseball cap. In this case, it took the group very little effort to counter the technology.

[10] See, for example, discussion in Office of National Drug Control Policy, "Measuring the Deterrent Effect of Enforcement Operations on Drug Smuggling, 1991-1999," August 2001.

[11] See, for example, discussion in Blas Nuñez-Neto and Stephen Viña, "Border Security: Barriers Along the U.S. International Border," Congressional Research Service, RL33659, September 21, 2006.

[12] See, for example, discussion in Nuñez-Neto and Viña, 2006.

Principles for Designing Defensive Technology Efforts

Given the costs of designing and implementing novel border security technologies, it is important to consider the threat that adversary adaptation poses to their eventual effectiveness and value during research, development, test, and evaluation planning, and implementation.[13] Looking across the terrorist groups we studied, we identified a number of principles that should be considered as next-generation measures are designed and implemented. In some cases, what our review of historical terrorist group behavior had to teach us was "not news": Some of the lessons merely reinforced the importance of principles already considered good practice in technology design and testing. However, in other cases, what they had to teach was less obvious. In all cases, the potential result of not learning the lessons is high: losing the opportunity to prevent terrorist attacks.

The Importance of Testing and "Red Teaming" Technologies

Terrorist groups' countertechnology efforts underscore the importance of extensively testing new security measures before they are introduced. To make sure new technologies will perform over time, designers need to assess what information adversaries would need to circumvent the technologies and identify how they might get access to that information. Can groups "test" a defense's capabilities by challenging it in different ways? If a measure's performance relies on keeping some details of its capabilities secret, how long can those secrets be kept? Furthermore, dedicated "red teaming" of new technologies—challenging them with teams of capable individuals to see if they can discover new ways to penetrate the security measures—is also critical. Such testing is established practice for many security technologies and measures. For example, when it comes to cybersecurity, companies routinely use "hackers" to challenge security measures the companies have put in place. The need to test new technologies and explore their possible weaknesses also suggests that small-scale technology demonstration projects and evaluation studies of promising technologies may be particularly valuable intermediate steps to include in technology programs whenever possible before they are expanded to larger-scale demonstration or technology-deployment efforts.

Maintaining Flexibility in Technology Design

Given that adversaries will almost certainly find ways to degrade the performance of even the best security technologies, we should preserve as much flexibility as possible in the technologies we design and deploy. If the design of a defensive measure locks it in to a single configuration or operating mode, its benefits are vulnerable to changes in adversary behavior. If the security

[13] Michael A. Wermuth and K. Jack Riley, "The Strategic Challenge of Border Security," Testimony Before the Committee on Homeland Security, Subcommittee on Border, Maritime and Global Counterterrorism, U.S. House of Representatives, March 8, 2007, available at http://www.rand.org/pubs/testimonies/CT275/

measure is static[14], it will not be able to adjust to a dynamic threat. In contrast, if flexibility is built into the defense from the start—e.g., if, when a terrorist group "breaks the code" on how the defense functions, we can change the code and reconstitute performance—then the benefits provided by the defensive measure can be preserved. Just as the terrorists we studied were able to change their operational practices to get around defensive technologies—e.g., obscuring the signatures they were designed to detect, using deception, adjusting the speed or character of their operations—changes in operational practices could similarly provide a variety of strategies for altering the character of defensive systems. For example, maintaining the ability to redeploy surveillance systems or change how security forces respond to alarms from detection systems are ways that technological performance could be altered to respond to changes by adversaries.

Systems that are flexible—that are not locked into specific modes of operation—preserve the opportunity for border security organizations to adapt their performance to respond to changes made by individuals and organizations seeking to enter the country illegally. Considering the value of this flexibility in the evaluation of potentially new technologies is important, since providing such flexibility may require additional expenditures up front when the defense is designed and implemented. If it is not considered, options that could provide robustness may be inadvertently sacrificed in an effort to reduce costs.

Developing Portfolios of Defensive Options for Defense in Depth

The risk that adversaries will identify strategies to defeat or evade individual security measures also suggests that the United States should maintain a diverse and flexible border security research, development, test, and evaluation portfolio. If we devote all our resources to optimizing a single line of defense, there will be no backup available if that line is breached. This is one reason behind the idea of defense in depth—maintaining multiple lines of protection against high-risk threats.

Security planners should consider a variety of defensive technology options, maintaining possibilities for alternative approaches if currently effective technologies are neutralized. Even if multiple defensive lines are not all deployed at the same time, a portfolio approach to developing defensive measures could provide "fall back" options if an initial defense becomes obsolete. Depending on the level of adaptive threat, the nation could be better off having multiple defensive options of average effectiveness than a single highly effective option without a viable back-up. If decisions are made to pursue a specific path, the costs of maintaining other technologies in

[14] Depending on the security measure, the technological characteristics—e.g., the nature of a detection technology—could make it difficult or impossible to change in response to adaptation by an adversary. In other situations, the combination of technology and the way it is used— e.g., including the concept of operations, etc.—could make it possible to respond to countermeasures.

reserve—perhaps not fully developed, but at a stage at which they might be called on if needed—should be considered as well. Such an approach is analogous to maintaining a diversified portfolio of investments, containing a variety of options, where comparatively small investments provide various hedges against different shifts in circumstances. Small-scale technology demonstration projects and evaluation programs can also help to pursue this strategy, since they can provide a cost-effective way to explore multiple security options and assess their relative performance and robustness.

Conclusions

When adversaries are successful in countering all or part of a defensive technology, the utility of the system may be significantly reduced or lost entirely. Such losses devalue the costs society pays to design, produce, field, use, and maintain the technology—where costs include not just financial and materiel costs but also less tangible costs such as reductions in privacy or the inconveniencing of individuals legitimately crossing U.S. borders, when such security measures are implemented. Given the scale of U.S. borders and the volume of individuals and goods that cross them everyday, those costs can be considerable.

As a result, "adaptive destruction" is one more risk that must be managed by the science and technology programs charged with developing novel border security capabilities. The potential that adversaries might break through a defense soon after its introduction must be assessed and included in the cost-benefit analyses that provide the basis for going forward with large-scale technology testing and procurement. Not doing so may lead to major investments whose eventual benefits may not justify their costs. The robustness of new defensive technologies against adversary adaptation must be explicitly considered in crafting a technology roadmap for next-generation border security technologies and in efforts to deploy current technologies on the borders.

Furthermore, although the focus of the discussion here is on technology, we must recognize how the technology choices we make affect the rest of the border security system and the how the interactions among the parts of that system shape the value of new technologies and defenses. Although an adversary's efforts to break through our defenses may be aimed at the technologies we use to protect ourselves, the impact of those efforts will be shaped by the concepts of operation around those technologies and the people charged with implementing them.

For example, if a new detection technology produces many false alarms (magnified perhaps by individuals or smuggling organizations intentionally triggering the sensors to undermine the value of the system) can such false alarms be dealt with quickly or will responding to them consume human resources that could be put to better use in other ways? If migrants and smugglers respond to border fencing and surveillance by regularly damaging the fence and its associated systems, how will a constant stream of repair efforts affect DHS's security efforts? If the defenses we deploy simply result in displacement (e.g., individuals shift from crossing the border at one location to another) are we better off, worse off, or the same from a security perspective?[15]

The answers to these questions depend not just on technology but on how all the elements of the border system work together, and their answers will partly determine how much of a threat adversaries' countertechnology efforts pose to the country.

Although technologies can provide an edge in protecting our borders, that edge can be dulled by adversaries' countertechnology efforts. An understanding of the way adversaries have responded to counter defensive technologies in the past underscores the complexity of designing new systems to protect society from the threat such adversaries pose. Our research suggests that, in designing protective measures, we should not immediately assume that the newest and most advanced technologies—the highest wall, the most sensitive surveillance—will provide the best protection. Drawing on common metaphors for defensive efforts, a fortress—relying on formidable but static defensive measures—is a limiting strategy. Once a wall is breached, the nation is open to attack. Depending on the adaptive capabilities of the adversary, a defensive model built from a variety of security measures that can be adjusted and redeployed as their vulnerable points are discovered provides a superior approach. However, whatever combination of models and measures is chosen, it is only by exploring adversaries' potential countertechnology behaviors that vulnerabilities in current and potential future defensive measures can be discovered and addressed.

I would like to thank you again for the opportunity to address the committee today on this important topic, and I look forward to answering any questions you might have.

[15] For example, diversion of illegal entry traffic from urban to rural areas has been characterized as beneficial from a security perspective, because individuals crossing the border in an urban area can vanish quickly into traffic, thus considerably reducing the time for apprehension. (David Aguilar, "Border Security: Infrastructure, Technology and the Human Element," Testimony Before the Subcommittee on Border, Maritime and Global Counterterrorism, Committee on Homeland Security, U.S. House of Representatives, February 13, 2007.)