Revamping of airport checkpoint system urged

By Anne E. Kornblut and Ashley Halsey III
Washington Post Staff Writers
Friday, December 17, 2010; 12:00 AM

Nine years after the Sept. 11 attacks and decades after hijackers first began to target passenger airliners, the United States has invested billions of dollars in an airport system that makes technology the last line of defense to intercept terrorists.

It has yet to catch one.

In every known recent attempt, terrorists have used a different tactic to evade the latest technology at airport checkpoints, only to be thwarted by information unearthed through intelligence work - or by alert passengers in flight.

The result is an emerging consensus among experts and lawmakers that the checkpoint-heavy approach - searching nearly every passenger - may not be the most effective.

Instead, many of them say, the system should focus more urgently on individuals, gathering a greater range of information about people to identify those most likely to present a real danger.

Scanners, pat-downs and bomb-sniffing dogs are all vital parts of the process but should be integrated into a multilayered system that includes far-reaching, computer-filtered data about people, along with face-to-face monitoring by the modern equivalent of a beat cop, several officials and experts said. Technology matters, they said, but it is akin to putting up a series of picket fences for terrorists to evade.

U.S. officials and lawmakers acknowledge that broader revisions may be necessary, saying it is only a matter of time before the airport security apparatus fails.

"Let's be honest: We've been lucky the last few times," said Senate Homeland Security Committee Chairman Joseph I. Lieberman (I-Conn.). "With the Christmas Day bomber over Detroit and the Times Square bomber and the air cargo attempt, they did not succeed, but that's because of their own inadequacies, not because we were able to stop them."

As a result of those attempts, passengers must surrender sharp objects (a response to the Sept. 11 attacks) and slip off their shoes (a response to the 2001 would-be shoe bomber). They must remove liquids from their bags (a result of a 2006 plot to blow up planes), and, as of a few weeks ago, they must submit to body scans or pat-downs (a process accelerated by the attempted airline bombing last Christmas Day).

Yet lawmakers and government reports question the capability of some specific measures. Year after year, undercover testers manage to sneak loaded weapons past screeners in embarrassing

evasions. More broadly, skeptics describe the extreme focus on airport checkpoints as incomplete, too often focused on the last attack rather than the next one.

Even Transportation Security Administration head John S. Pistole, in an interview, described his agency as merely a "last line of defense on a continuum of government national security efforts."

Like others interviewed, Pistole said he hopes to move to a more intelligence-based system, but said the previous attacks could never be ignored.

"We always have to look out for yesterday's threats," he said. "Shame on us if there's ever a repeat of 9/11 or the shoe bomber or the underwear bomber, if we haven't hardened our targets."

Some critics have given the labyrinthine airport security system the nickname "security theater," saying it is riddled with loopholes. Airport workers are not screened daily, making them capable of passing into secure areas with weapons. Lines inside the terminal are vulnerable to a would-be suicide bomber. Packages sent as cargo go through a comparatively light screening process - one that is being tightened but was exploited by al-Qaeda operatives in October when they sent bombs hidden in printer cartridges.

"After 9/11, the attacks failed because of the poor skills of the terrorists rather than anything we've done," said Rafi Ron, former security director at Tel Aviv's Ben Gurion International Airport. "In every one of these later attacks, the security checkpoint was overcome by terrorists who took advantage of the loopholes."

For al-Qaeda, forcing the United States to continually add layers of air security amounts to victory in its own right. "If your opponent covers his right cheek, slap him on his left," its writers gloated in the organization's magazine, Inspire. "The continuous attempts that followed 9-11 . . . have forced the West to spend billions of dollars to defend its airplanes." The strategy, they wrote, is one of "a thousand cuts" to "bleed the enemy to death."

The repeated attempts have pushed U.S. officials into a costly pattern of trial and error, testing what works - and what the public will accept. Since 2002, the TSA budget has totaled $57.2 billion - about what the government spends on intelligence programs in a single year. Still, there have been obvious aviation excesses.

Machines, such as the $160,000-a-pop "puffer portals" introduced in 2004, have been introduced and then jettisoned. The color-coded terrorism alert program is on its way out. Britain plans to abandon its restrictions on liquids in April, and U.S. officials say they would like to do the same, although they question whether it's too soon.

Other changes may soon follow. Rep. John L. Mica (R-Fla.) wants to replace TSA workers with private screeners, as 17 airports nationwide have done, to make them more efficient and accountable. Others would shift to a system that incorporates more passenger data into the screening system, on top of the new identity markers - including a passenger's sex and birthday - that airlines recently started to gather.

More immediately, Pistole said he wants to see modifications to the scanning machines that caused such an uproar, "so you see a stick figure of the blurred image versus the, quote, 'naked photos,' " he said. The new technology is being tested but yields too many false positives to be used, he said.

Even the system's fiercest advocates acknowledge its imperfections, saying alterations are almost certain. "Nothing's perfect. The strategy is evolving, and it's a work in progress," said Rep. Peter T. King (R-N.Y.), the incoming chairman of the House Homeland Security Committee. "We're fighting the last war; we're trying to anticipate the next war. There's inconvenience. Some things have worked; others haven't. There's no silver bullet."

He added: "But let's face it: We haven't been attacked. If anyone back on September 12, 2001, would have said we'd go eight, nine years without a successful aviation attack, no one would have believed them."

Fighting the last war

Whether the new patchwork system deserves credit for the stability of the past nine years is up for debate. Although none of the dozens of suspected terrorists arrested in the United States during that time were caught at aviation checkpoints, it is impossible to know how many were deterred by airport security from even trying. Several took aim at softer targets: New York subways, as in the case of Najibullah Zazi, or a car in Times Square, as in the case of Faisal Shahzad.

But would today's mechanisms even block a future Umar Farouk Abdulmutallab? The question troubles security experts, who see persistent flaws - from gaps at checkpoints for flights originating overseas, as Abdulmutallab's did, to problems with the way full-body scanners work.

The advanced imaging technology scanners were in use at 19 airports when Abdulmutallab allegedly tried to ignite explosives in his underwear on Christmas Day last year as his flight from Amsterdam landed in Detroit. The administration accelerated the machines' rollout, to 500 nationwide by this Christmas, in case someone tries the same tactic domestically.

Some critics question whether the machines expose travelers to too much radiation. Even more are concerned about the technology's intrusiveness and whether the method will work. According to independent analyses, it would not detect explosives placed deep inside a body cavity or in large rolls of body fat.

"It remains unclear whether the AIT would have detected the weapon used in the December 2009 incident," said a Government Accountability Office report in March.

"If you're hiding something in an orifice, that's hard to detect," said Vahid Motevalli, head of the department of mechanical engineering technology at Purdue University.

Senior U.S. officials played down those concerns, saying that in order for a bomb to explode properly it must be close to the body's surface. The body acts as "a retardant for the explosion," said one senior official, who spoke on the condition of anonymity so he could discuss security issues freely. Therefore, it is unclear whether body-cavity bombs will become the wave of the future.

Although profiling carries the burden of a racist history in the United States, a more sophisticated version is an integral part of the Israeli model. Israeli profiling targets more than Palestinians, Arabs or Muslims, though they may receive the closest scrutiny. The most widely celebrated example was the interception in 1986 of Anne-Marie Murphy, 32, who was six months pregnant when she attempted to board an El Al flight from London to Tel Aviv, unaware that her fiance had placed a bomb in her bag.

Experts say the United States is unlikely to adopt the Israeli model. It "includes ethnical and national profiling, " said Ron, the former Israeli airport security director. "Being a Palestinian in Israel is not an advantage, obviously. In the U.S., any ethnical or national profiling is illegal or unacceptable for the American public."

But more than a dozen U.S. officials, lawmakers and experts interviewed said they would like to move to a system that relies more on passenger data than on airport checkpoint screening.

"I would like to see a lot more profiling," said the Israeli-born Yossi Sheffi, who is an expert on risk analysis and directs the Massachusetts Institute of Technology Center for Transportation and Logistics.

"If you're tall and dark and going to Yemen and your name is bin Laden, you should be searched more than an old grandmother from Kansas City with a walker," he said.

But as the recent furor - albeit temporary - over the full-body scanners illustrated, there are obstacles to introducing new measures, especially those that invade privacy.

After Sept. 11, 2001, the George W. Bush administration proposed a $380 million program that would have combined commercial data about passengers with flight manifests to give a more complete picture of travelers. Civil liberties groups objected and the program was dropped, but some now say it might make sense to consider a revised version.

Department of Homeland Security officials already have access to some commercial data about passengers traveling from overseas. But if the security system were allowed to access even more - such as personal information collected by companies that do credit ratings - suspicious passengers would be more readily identified, experts say.

Asked whether he would be open to revisiting that idea, Pistole replied: "Sure, if Congress said we should do that."

"Honestly, the more we know about a person, the more informed we can be and the more intel-based approach we can use the better," he said. "But it just comes down to civil liberties, privacy, all those hot-button issues."

Rep. Bennie Thompson (D-Miss.), the outgoing chairman of the House Homeland Security Committee, also said he would be open to collecting more commercial data, and King, the incoming chairman, agreed. But, Thompson said, concerns about civil liberties remain a "delicate balance."

"I'd be open to looking at it," Lieberman said. "You have to give some weight to privacy concerns, but I wouldn't close the door to it."

kornbluta@washpost.com halseya@washpost.com

Staff researcher Julie Tate contributed to this report.