TSA: Mission Creep Meets Waste

Hal Berghel, University of Nevada, Las Vegas

The acronym TSA could just as well stand for "tactics to suppress accountability." It's an object lesson in the misuse of technology toward ill-defined ends.

Mass media regularly feeds on the Transportation Security Administration (TSA)'s checkered past, and for good reason. According to a recent ABC News exclusive, "an internal investigation of the Transportation Security Administration revealed security failures at dozens of the nation's busiest airports, where undercover investigators were able to smuggle mock explosives or banned weapons through checkpoints in 95 percent of trials."[1] This followed the leak of an internal Department of Homeland Security (DHS) inspector general's report indicating that TSA agents failed to detect 67 out of 70 threats presented by red team members. This isn't an isolated problem at the TSA, as we'll see. DHS secretary Jeh Johnson's response was to announce some insubstantial changes and re-assign the TSA director.[2] As is the way with government, oversight of the internal investigation and change process will fall to a team of DHS and TSA insiders, as these are the tools that bureaucrats use to diffuse criticism or cover up problems.

What's more, the DHS inspector general (IG) announced a few days later on 9 June 2015 that he has launched an investigation into the source of the leak(s) exposing the TSA's ineffectiveness in detecting guns and bombs in the first place.[3] In the span of two weeks in early June the DHS went from imbalanced defense to full-court offense: it silenced the media and Congress by announcing a sham investigation, while aggressively pursuing the whistleblowers who brought the public's attention to the matter—that's a great way to send a very clear signal to TSA agents who might be inclined to talk to reporters or Congress.

It is axiomatic in government that the way to make an ineffective program work better is to make it larger. Axioms, of course, are assumed and not proven. The TSA's approach to this was to create added screening programs such as the Visible Intermodal Prevention and Response (VIPR) squads.[4] These VIPR squads were another byproduct of the George W. Bush administration's concession to bigger government. But after three years of operation, the 2008 DHS IG reported that more than 50 percent of VIPR inspectors surveyed didn't understand their mission, chain of command, or job responsibilities.[5] After such a glowing review, the criticisms of VIPR teams for harassment of the traveling public must have come as quite a shock to Congress.[6]

0018-9162/15/$31.00 © 2015 IEEE

Four years later, the DHS IG reported that the VIPR program's problem was that it lacked an effective public relations campaign and the employees didn't know how to prepare reports—where's Edward Bernays when we need him?[7] These IG reports suggest that this swine needs more lip gloss.

AND THE BEAT GOES ON

But there's more. The TSA also introduced the Screening of Passengers by Observation Techniques (SPOT) program that uses Behavioral Detection Officers (BDOs) to identify potential security risks by "identifying behaviors and appearances that deviate from an established baseline and that may be indicative of stress, fear, or deception." This ignores whether any of the aforementioned behaviors could have been induced by amateurish and nonsensical TSA rules, long lines at security checkpoints, the presence of armed VIPR agents in public areas suggestive of banana republics, or, heaven forbid, impolite TSA agents. By any objective measure it's an open question whether SPOT accomplishes anything toward the goal of thwarting terrorism that would justify its existence.

In its first year of operation, SPOT detained 50,000 passengers for additional screening, and 3,600 of these were referred to law enforcement. Of these 3,600 incidents, "… 27 percent were illegal aliens, 17 percent were drug related, 14 percent were related to fraudulent documents, 12 percent were related to outstanding warrants, and 30 percent were related to other offenses."[8] Not one terrorist to be found in this dragnet. Some of you might recognize the similarity between these results and those reported by the NSA to Congress on its bulk metadata collection program.

The 26 March 2012 Government Accounting Office (GAO) report to Congress was particularly illuminating.[8] In one attempt to validate SPOT, DHS's independent panel of investigators determined in April 2011 that "SPOT was more effective than random screening to varying degrees." This was even after the BDOs had been made aware that the suspected individuals were already flagged as a potential risk by earlier screenings. This is government science at its finest: we tell you in advance that the subjects are thought to pose a risk, and then your subsequent confirmation of that fact is as likely to be accurate as a coin toss. Anyone who thinks that this is tax money well spent is delusional.

In fact, SPOT officials admitted they didn't know if the program resulted in the arrest of any terrorists or those planning to engage in terrorist-related activity.[8] In a left-handed attempt to defend TSA performance, the GAO noted that the TSA is only attempting to measure output (at which it fails miserably, incidentally), whereas the Office of Management and Budget (OMB) encouraged the use of "outcome measures—which track progress toward a strategic goal by documenting the beneficial results of programs—because they are more meaningful than output measures. …"[8] That's government speak for "break out the smoke and mirrors"—there has been no serious attempt to determine whether anything important has been accomplished.

After years of bad press, the TSA abandoned the scanners because—hold on to your seats for this one—they didn't work.

Neither outcomes nor output assessment can confirm any SPOT successes. The GAO also noted that the DHS failed to complete a cost-benefit analysis before deployment. So there you have it: the DHS didn't try to justify SPOT as a good idea before it launched, and then it failed to seriously study whether anything useful resulted. That's what bureaucrats and government contractors call a home run.

It also must be understood that the GAO, as part of the US government, is inclined to support other agencies, rather than condemn them. Independent analyses of TSA programs, rare as they are, are far less optimistic than the GAO's. For example, in 2014 the first independent analysis of the advanced imaging technologies (AIT) backscatter x-ray body scanner (https://radsec.org/secure1000-sec14.pdf, p. 13) found it to be "ineffective as a contraband screening solution against an adaptive adversary." The authors documented that it's relatively easy to conceal weapons, explosives, and detonators using concealment tactics of positioning, masking, and shaping. This confirmed the Electronic Privacy Information Center's (EPIC's) warnings from 10 years earlier.[9]

The TSA is yet another privacy-invading, tax-wasting, make-work jobs program with an ill-defined mission and no end-game strategy thrown into the military–industrial–surveillance–political–media–prison–Wall Street–banking–energy–healthcare–academic–think tank–corporatist–homeland security–prohibitionist–carbon-combustion complex. Such programs are the stuff of which geriatric empires are made.

GETTING IT WRONG

Unfortunately, most travelers fail to look beyond their frequent irritation when thinking about the TSA, and that lack of public furor gives the TSA license for most of the waste and abuse. There are no incentives for transparency and accountability. This is now so far out of control that EPIC is holding conferences on the subject (https://epic.org/events/tsa). Thus far, the TSA and DHS are allowed to remain passive with respect to negative scientific and media reports, precisely because their overseers are beholden to government contractors and lobbyists, not media or civil libertarian groups. Some examples of notable TSA blunders include the backscatter x-ray body scan, the botched handling of the no-fly list, electronic randomizers, and other notable misses.

The backscatter x-ray body scan

What a classic example of going from sublime to ridiculous. Early on, we learned that these revealing digital images held prurient appeal.[10] Somehow it never occurred to the TSA that these racy digital images might take flight from the scanner. It wasn't long until those "images of interest" became digital currency.[10,11] But those expensive scanners maintained a high burn rate, and that made both the government and its contractors happy—it's sometimes hard to tell the two groups apart.[12] After years of bad press, the TSA abandoned the scanners because—hold on to your seats for this one—they didn't work. It seems that C-4 explosives and human flesh register the same on the scanners.[13] The technology wasn't scientifically tested for effectiveness in the real world, and it was known not to work before it was even deployed. As of this writing, the scanners are reserved for use with controlled populations like prisons.

It's important to emphasize that body scanners were always opposed on constitutional grounds,[14] and they were never scientifically proven to work, as shown by the underwear bomber.[15] The fact that the TSA confiscates pen knives and beverages while allowing a person wearing explosive underwear to board did little for its credibility. In 2013, the GAO reported that there was no evidence of SPOT's effectiveness in identifying aviation threats and recommended that Congress and the president withhold funding.[16]

I label programs like those described here as "faith based"—recognizing the only measure of effectiveness that they satisfy.

Bungling the no-fly list

The TSA's and DHS's involvement in the no-fly lists of various types (projects like the computer-assisted passenger prescreening system [CAPPS I and CAPPS II], Selectee [SSSS] List, Secure Flight, and others) have been controversial since inception. The problem is that the selection criteria for inclusion aren't known and are thus unavailable for testing. There's never been significant public debate on the topic. The only way to know that you're on one of these lists is to be stopped at a security checkpoint. Such was the case with Senator Ted Kennedy,[17] but unlike Kennedy, most travelers don't have the president's or US cabinet officials' cell phone numbers, nor any effective recourse. (As an aside, after Kennedy's no-fly list experience, George W. Bush canceled the CAPPS II program that caused it.)

As far as I know, there's no real opposition to the use of watch lists as long as the membership isn't politically or ideologically motivated, random, or arbitrary. There's considerable evidence that these lists are used as much for harassment as security. It should be pointed out that Nelson Mandela was on a no-fly list until Secretary of State Condoleezza Rice had him removed in 2008. Underwear bomber? No. Nelson Mandela? Yes. We can't blame this on false positives as some would have you believe (https://en.wikipedia.org/wiki/No_Fly_List), but rather on bogus algorithms. This isn't a system with a Type I error, but a system that is Type I stupid.

Electronic randomizers

In an effort to prevent passengers' self-selection of screening conveyor belts in airport security areas, the TSA recently had the brilliant idea that such assignments should be randomized and issued a request for information.[18] Let's think about this. What drives a traveler's inspection station selection? A compromised TSA agent spotted on a particular line, revealing a terrorist opportunity? Unlikely. More likely, however, is that the line is moving faster! Such being the case, the traveling public might see this as a way to randomly assign passengers to slower and longer lines, and therefore it won't be warmly received.

We need only to look to the developing world to find a randomizing technique that meets public acceptance. Everyone approaches the security checkpoint, shows their credentials, and pushes a giant button on a small traffic light at the end of the belt. Green: good to go. Red: you get everything inspected manually. We could even add orange: empty your pockets and place their contents and your bags on the belt to go through the x-ray machine. Mexico used a system like this for decades. The cost is a few old traffic lights, a big button, a pole, and a few relays. Mexico understood that terrorists don't need to think that the chance of getting stopped is 100 percent to be dissuaded. They only need to believe that the chances are significant. The fact that they might get arrested is the deterrent.

Loath to loathe

My point is that frequent travelers have come to loathe the TSA for the wrong reasons. If an expensive suit is ruined because a sloppy TSA agent closed the bag with a sleeve hanging out, we internalize the irritation and go about our business. What we should do is contact our congressional delegation and demand that accountability and transparency be imposed on the TSA. In the case of the suit, adding accountability is trivial: the TSA inspection sticker should have a barcode representation of a one-way hash of the inspector's employee, location, and timestamp information. That would be enough information for the TSA to monitor the complaints without disclosing personnel information to the traveling public. If one inspector averages many complaints per day, that should trigger some management action. As things now stand, the public is loath to demand accountability, so none is required. The TSA isn't just an annoying and pointless government activity, it's an insidious invasion of privacy that's only occasionally accidentally effective in stopping terrorism.

OTHER DARK TSA MOMENTS

There are, of course, more TSA gaffes than there is space to cover here, but here are some honorable mentions, without comment, for your consideration.

- The TSA missed 73 terrorism-flagged airline workers (www.politico.com/story/2015/06/tsa-missed-73-terrorism-flagged-airline-workers-report-118738.html).
- The TSA doesn't maintain its equipment properly (http://dig.abclocal.go.com/wls/documents/TSA%20equipment%20OIG.pdf).
- The TSA is ineffective at badge, ID, and uniform management (www.securityinfowatch.com/news/10501495/tsa-responds-to-inspector-general-over-badge-concerns).
- The TSA spent nearly US$500,000 on a birthday party and awards banquet to boost morale (www.washingtonpost.com/wp-dyn/articles/A2399-2005Apr19.html).
- TSA audits reveal problems (http://chsdemocrats.house.gov/SiteDocuments/20110803172118-83003.pdf).

FAITH-BASED SECURITY

I prefer to label programs like those described earlier as "faith based" in recognition of the only measure of effectiveness that they satisfy.[19] The longevity of faith-based programs is a function of how successfully they shun relevant science and impartial third-party oversight, and their ability to cater to the demands of what President Eisenhower called the military–industrial complex. President Reagan's Strategic Defensive Initiative (SDI or Star Wars) was one noteworthy example of a faith-based security program. Championed by CIA director William Casey and deputy director Robert Gates, and aided by a collection of neoconservative ideologues within the intelligence and defense communities, this science-fiction solution to an external missile threat was widely discredited by the scientific community as unworkable from the get-go.

Many of us recall David Lorge Parnas's famous article on the subject, "Software Aspects of the Strategic Defense Systems."[20] SDI was also vilified as a waste of taxpayer money,[21] and by some objective accounts, missile defense that began under Reagan cost the taxpayer in excess of US$200 billion[22]—with no end in sight.[23,24] This is exactly what former Soviet president Mikhail Gorbachev predicted. He told Reagan, "I think you're wasting money. I don't think it [SDI] will work. But if that's what you want to do, go ahead."[21] Star Wars' strongest support came from retired physicist Edward Teller, big and powerful government neoliberals and neoconservatives, and perhaps Nancy Reagan's astrologers, yet the concept refuses to die. The allure of all those unauditable tax dollars is just too much for the military–industrial complex to overlook.

Faith-based programs like the TSA, the Federal Emergency Management Agency (FEMA), SDI, DHS fusion centers, Northern Command (Northcom), and the like must operate without oversight because oversight would expose the fact that they don't work as intended. That's the prime motivation for overclassifying these programs and the paperwork they generate. Ribald claims of effectiveness are made and conclusions are intuited. But no hypotheses are tested, no evidence is adduced, statistical modeling isn't even discussed, and the academic science and engineering community—groups that actually have something significant to bring to the table—aren't consulted. Behind every faith-based security program is a cozy government-inspired political valence. This is the real heart of the problem.

So, the next time the TSA forces you into the longest line or ruins one of your expensive garments, you're left with only your faith that this inconvenience serves a greater good. The alternative would be to encourage a national public discussion. I've just done my part; the rest is up to you.

REFERENCES

1. J. Fishel et al., "Undercover DHS Tests Find Security Failures at US Airports," *ABC News*, 1 June 2015;

http://abcnews.go.com/ABCNews/exclusive-undercover-dhs-tests-find-widespread-security-failures/story?id=31434881.

2. "Statement by Secretary Jeh C. Johnson on Inspector General Findings on TSA Security Screening," announcement, Dept. of Homeland Security, 1 June 2015; www.dhs.gov/news/2015/06/01/statement-secretary-jeh-c-johnson-inspector-general-findings-tsa-security-screening.
3. A. Halsey, III, "Homeland Security Looks for Leaker of Report on Airport-Checkpoint Failures," *The Washington Post*, 9 June 2015; www.washingtonpost.com/local/trafficandcommuting/homeland-security-looking-for-leaker-of-report-on-airport-checkpoint-failures/2015/06/09/570ede22-0eb3-11e5-adec-e82f8395c032_story.html.
4. "Visible Intermodal Prevention and Response (VIPR)," announcement, Office of Law Enforcement/Federal Air Marshal Service, Transportation Security Agency, updated 25 June 2015; www.tsa.gov/about-tsa/visible-intermodal-prevention-and-response-vipr.
5. *TSA's Administration and Coordination of Mass Transit Security Programs*, audit report, Office of Inspector General, Department of Homeland Security, June 2008; www.oig.dhs.gov/assets/Mgmt/OIG_08-66_Jun08.pdf, p.63.
6. R. Nixon, "TSA Expands Duties beyond Airport Security," *The New York Times*, 5 Aug. 2013; www.nytimes.com/2013/08/06/us/tsa-expands-duties-beyond-airport-security.html.
7. *Efficiency and Effectiveness of TSA's Visible Intermodel Prevention and Response Program within Rail and Mass Transit Systems*, report, Office of Inspector General, Department of Homeland Security, Aug. 2012; www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-103_Aug12.pdf, p. 16.
8. S.M. Lord, *Progress and Challenges Faced in Strengthening Three Key Security Programs*, statement to the Government Accountability Office, 26 Mar. 2012; www.gao.gov/assets/590/589587.pdf, p. 8.
9. *Spotlight on Surveillance: Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding*, Elecronic Privacy Information Center, June 2005; https://epic.org/privacy/surveillance/spotlight/0605.
10. J.E. Harrington, "Dear America, I Saw You Naked," *Politico*, 30 Jan. 2014; www.politico.com/magazine/story/2014/01/tsa-screener-confession-102912_full.html.
11. D. McCullagh, "Feds Admit Storing Checkpoint Body Scan Images," *CNET*, 4 Aug. 2010; www.cnet.com/news/feds-admit-storing-checkpoint-body-scan-images.
12. K. Kindy, "Ex-Homeland Security Chief Head Said to Abuse Public Trust by Touting Body Scanners," *The Washington Post*, 1 Jan. 2010; www.washingtonpost.com/wp-dyn/content/article/2009/12/31/AR2009123102821.html.
13. A. Greenberg, "Researchers Easily Slipped Weapons Past TSA's X-Ray Body Scanners," *Wired*, 20 Aug. 2014; www.wired.com/2014/08/study-shows-how-easily-weapons-can-be-smuggled-past-tsas-x-ray-body-scanners.
14. A. Welch, "Full-Body Scanners: Full Protection from Terrorist Attacks or Full-On Violation of the Constitution?," *Transportation Law J.*, vol. 37, no. 3, 2010, pp. 167–198; www.law.du.edu/documents/transportation-law-journal/past-issues/v37-03/Welch-Body-Scanners.pdf.
15. USA v. Umar Farouk Abdulmutallab, Indictment, US District Court, Eastern District of Michigan, Case 2:10-cr-20005-NGE-DAS; www.cbsnews.com/htdocs/pdf/Abdulmutallab_Indictment.pdf.
16. *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, report GAO-14-159, US Government Accountability Office, 8 Nov. 2003; www.gao.gov/products/GAO-14-159.
17. "Kennedy Has Company on Airline Watch List," *CNN*, 20 Aug. 2004; www.cnn.com/2004/ALLPOLITICS/08/20/lewis.watchlist/index.html.
18. "TSA Will Use Electronic 'Randomizers' to Randomly Route Passengers to Screening Lines," *Government Security News*, 9 Jul. 2013; www.gsnmagazine.com/node/30506?c=airport_aviation_security.
19. H. Berghel, "Faith-Based Security," *Comm. ACM*, vol. 51 no. 4, 2008, pp. 13–17.
20. D.L. Parnas, "Software Aspects of Strategic Defense Systems," *Comm. ACM*, v. 28, no. 12, 1985, pp. 1326–1335.
21. M. Goodman, *National Insecurity: The Cost of American Militarism*, City Lights Books, 2013, chapter 7.
22. S.I. Schwartz, "The Real Price of Ballistic Missile Defenses," *WMD Junction*, 13 April 2012; http://wmdjunction.com/120413_missile_defense_costs.htm.
23. "Ronald Reagan's 'Star Wars' Project Still Hasn't Met Original Goal 30 Years Later," *Raw Story*, 23 May 2013; www.rawstory.com/2013/05/ronald-reagans-star-wars-project-still-hasnt-met-original-goal-30-years-later.
24. G.N. Lewis and T.A. Postol, "A Flawed and Dangerous U.S. Missile Defense Plan," Arms Control Assoc., 5 May 2010; www.armscontrol.org/act/2010_05/Lewis-Postol.

HAL BERGHEL is an ACM and IEEE Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.