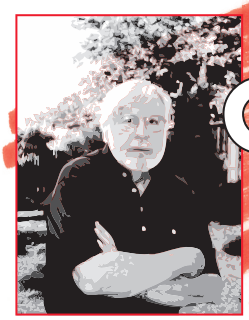

Outside the Lines

Problems cannot be solved by thinking within the framework in which the problems were created." – Albert Einstein

by Ludwig Benner, Jr. and Ira J. Rimson

Déjà Vu All Over Again-- An Opportunity for Us

"The shark's appetite for blood will not be converted into the hunger of goldfish, easily satiated with little crumbs."
— Stanley Crouch, syndicated columnist

Four years ago in this publication, we titled our column "When Safety Depends on Security."[1] We described the breakdown of security at an ATF[2]-approved storage facility that enabled the theft of large quantities of explosives, detonator cord and blasting caps. Thieves had stolen 350 pounds of ammonium nitrate[3] from that same "ATF-approved" facility just 25 months before. Neither the ATF nor its "approved" local licensee apparently had learned the lesson from the first event well enough to avoid the occurrence of the second.

We recently had occasion to recall those events after Umar Farouk Abdulmutallab, an ineffectual Islamist wanna-bomber, attempted to initiate an explosion aboard Northwest Airlines (NWA) Flight 253 en route from Amsterdam to Detroit Metropolitan Airport.[4] The pentaerythritol tetranitrate (PETN) plastic explosives that he had concealed in his underwear failed to detonate. The only injuries were burns to the attempted bomber and to the passengers who subdued him.

Why do we title this column "Déjà Vu All Over Again?" Let's start with the original subtitles and compare them with the current incident:

Original Subtitle 1: "How Could They Steal My Explosives? They Were in Approved Storage!"
Current Subtitle 1: "How Did He Get On the Airplane? We Have Approved Screening Techniques!"

The U.S. Department of Homeland Security (DHS) was established by the Homeland Security Act of 2002 (HSA).[5] The first two stated missions of the DHS are:

(1)(A): "prevent terrorist acts within the United States"

(1)(B): "reduce the vulnerability of the United States to terrorism."[6]

Within DHS, the Under Secretary for Border and Transportation Security's primary stated responsibility is:

(1) Preventing the entry of terrorists and the instruments of terrorism into the United States.[7]

Abdulmutallab's travels through Africa and the Middle East prior to boarding the initial flight leg from Lagos, Nigeria, have been well documented. His purchase of a one-way ticket to Detroit — in cash in Ghana — apparently aroused no suspicion (Strike 1). When he showed up for the KLM flight from Lagos to Amsterdam with no luggage for "a two-week stay in Detroit," he was passed through security screening without question (Strike 2). He received a similar pass from Dutch security at Schiphol Airport, enabling him to board the NWA

---

[1] *Journal of System Safety*, V. 42, No. 2, pp. 8-10, March-April 2006.
[2] Federal Bureau of Alcohol, Tobacco, Firearms and Explosives.
[3] A high explosive when mixed with fuel oil.
[4] See, e.g., http://en.wikipedia.org/wiki/Northwest_Airlines_Flight_253, *inter alia*.
[5] Public Law 107-296, 107th Congress.
[6] HSA, Section 101(b).
[7] HSA, Section 402.

flight to Detroit[8] (Strike 3). So much for "approved screening techniques."

Original Subtitle 2: "We Were Lucky, or, Were We Lucky?"
Current Subtitle 2:
(No Change Needed)

DHS was lucky. DHS was lucky that the techniques employed by Abdulmutallab and his Yemenite handlers were insufficient to detonate the explosives in his skivvies. The three ounces of PETN he wore was 50 percent more than the 50 grams (2 oz.) that Al-Qaeda member Richard Reid[9] tried to detonate on American Airlines Flight 63 on December 22, 2001. The NWA attempt was a retrocursor[10] to that failed attempt to ignite PETN aboard a U.S.-bound aircraft. DHS's response to the lessons that should have been learned from Reid's attempt was ineffectual. DHS was doubly lucky; had Abdulmutallab's mission been successful, DHS would have been hard put to explain it away.

Passengers aboard NWA Flight 253 were lucky. Abdulmutallab occupied seat 19A, a "window" seat. Tests after the Reid attempt demonstrated that 50 grams of PETN had sufficient explosive power to breach the skin of a transport airplane. Abdulmutallab had 50 percent more. NWA 253 had started its descent into Detroit when the detonation was attempted. It's likely that the force of the explosion, coupled with the remaining cabin pressure differential, would have caused destructive damage.

Residents under NWA Flight 253's flight path were lucky. Had Abdulmutallab been successful in his quest, the remains of the Airbus-330 and its 289 occupants would have rained down on persons and property below. Reconstruction of the flight path put the plane over western Ontario at the time of the attempt. That slight geographic discrepancy would not have gotten DHS off the hook for Abdulmutallab's being on the flight in the first place.

The country was lucky. Or maybe we weren't so lucky after all. Abdulmutallab's attempted bombing was likely ill-planned rather than random. After Reid's attempt, the TSA countered by requiring all potential airline passengers to remove their shoes for scanning. Yet the absence of more attempts at shoe-bombing in the interim eight years has been attributed more to terrorists' learning from the reactions that followed Reid, than to their success. The NWA 253 event once again revealed the TSA's dubious prevention efficacy against future terrorism attempts (Strike 4). Our government doesn't seem to understand that the objective of terrorism is not necessarily to destroy, but to invoke the threat of it to provoke terror. How else to explain the Justice Department's limiting Abdulmutallab's interrogation to a mere 50 minutes before permitting him to "lawyer up?" (Strike 5).

Original Subtitle 3: "The Fallacy of Mistaking Managerial Doublespeak for Action"
Current Subtitle 3:
(No Change Needed Here Either)

The day after Abdulmutallab tried and failed to detonate the PETN, DHS Secretary Janet Napolitano assured the world that "[T]he [aviation security] system worked." The resultant worldwide incredulity barely began to subside when she invoked the common bureaucratic bungler's *mea culpa* by saying that she had "been taken out of context," and that the real in-context meaning was, "Our system did not work in this instance." Subsequent instances of the system's not working occurred almost weekly thereafter.

Original Subtitle 4:
"Putting Spin on Fecklessness"
Current Subtitle 4:
(No Change Here Either)

How well has the DHS/TSA accomplished the missions we stated?

1. Has it "prevented terrorist acts within the United States?" A U.S.-flag air carrier is an image of U.S. sovereignty. Abdulmutallab's attempt was a terrorist act, whether successful or not. His intent was not necessarily to destroy the airplane and passengers, but to provoke terror at the inadequacy of the aviation security system.
2. Has it "reduced the vulnerability of the United States to terrorism?" The ease with which DHS/TSA's approved screening techniques were breached is an object lesson in fecklessness. TSA's security measures have been reactive. It has collected hundreds of thousands of nail clippers, shampoo and mouthwash bottles and Swiss Army knives — and in the process inconvenienced and antagonized millions of passengers — while doing nothing to improve security. More restrictions will surely be imposed now, even

---

[8] KLM and NWA are "code share" airlines.
[9] The "Shoe Bomber."
[10] See "The Curse of the Retros," *Journal of System Safety*, V. 45, No. 4, July-August, 2009.

"Safety depends on security. Traditional system safety applications have assumed that systems under study are secure from deliberate corruption. That is no longer the case. We cannot afford to wait for potential destroyers to play their hands before generating counteractions, hoping in the meantime that the system can survive the risk."

though existing screening techniques would have prohibited the terrorist's boarding, had they been applied. DHS/TSA cannot assure us that risks of similar breaches have been reduced. The NWA 253 incident has proved that terrorists think well ahead of DHS and TSA.

Original Subtitle 5: "Considerations for the System Safety Community"
Current Subtitle 5: (Same Here, Too)

The risks of deliberate attempts to penetrate the integrity of security systems are much greater than those inherent in mistakes or failures. That is all the more reason to subject vulnerable systems to detailed security analyses to determine weaknesses that could provide access to those bent on destruction. Safety depends on security. Traditional system safety applications have assumed that systems under study are secure from deliberate corruption. That is no longer the case. We cannot afford to wait for potential destroyers to play their hands before generating counteractions, hoping in the meantime that the system can survive the risk.

We wrote four years ago: "Expanding the 'hazard' side of the equation to include deliberate acts should not present a hurdle to applying traditional system safety methodologies. What *will* change is the traditional practice of converting those concepts into probabilistic assessments." When "failure" results from deliberate sabotage; probability = 1 and severity = destruction.

Recent evidence of the nation's cybersystems' pregnability to deliberate attack are an opportunity to expand system safety beyond its traditional roles.[11] More than 70,000 breaches of cybersecurity were reported by the DHS in 2008. Many occurred to control systems for the country's electrical grid, posing threats to the safety of all systems that depend on electrical power for control and management. The nation's water sources are equally at risk.

Similar vulnerabilities exist in the country's food supply system, especially now that large quantities are imported from worldwide sources. Terrorists need not penetrate our borders to contaminate U.S.-bound foodstuffs biologically or chemically.

These systemic insecurities are opportunities for applying system safety's 50 years' experience to bear proactively against credible hazards that currently face the nation. We must broaden our traditional mindset to enable us to apply that hard-earned knowledge to expanding our role effectively. Unearthing systems' vulnerabilities and protecting against deliberate attempts to cripple or destroy their security demands that system safety practitioners cultivate the "requisite imagination"[12] needed to think outside our traditional box.

In one way, the job has been made easier: We won't have to concern ourselves with traditional system safety "numerology." Where terrorism is concerned, P=1, and S=100%. Beyond that, there's unlimited opportunity.

---

[11] See, e.g., Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies." *Wall Street Journal*, April 8, 2009.
[12] See, e.g., Adamski, A. & Westrum, R. "Requisite imagination. The fine art of anticipating what might go wrong." In E. Hollnagel (Ed.), *Handbook of Cognitive Task Design* (pp.193-220). Mahwah, NJ: Lawrence Erlbaum Associates, 2003.