

The Atlantic

Is America Any Safer?

By Steven Brill

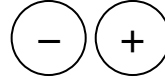
Since 9/11, the United States has spent \$1 trillion to defend against al-Qaeda and ISIL, dirty bombs and lone wolves, bioterror and cyberterror. Has it worked?

Photograph by Greg Kahn / A member of the NYPD's counterterrorism unit stands guard near the Brooklyn Bridge in New York City, July 4, 2016.

STEVEN BRILL

SEPTEMBER 2016 ISSUE | POLITICS

TEXT SIZE



Sections

I

II

III

IV

V

VI

FIFTEEN YEARS AGO this September 11, 19 terrorists, using four jetliners as guided missiles, killed 2,977 people—and enveloped the country in fear. It was the first sustained attack on American soil since the bombing of Pearl Harbor, which was a far-off military base. This massacre hit the center of our government and blasted away part of our most iconic skyline. It left a stench that New Yorkers could smell weeks later as remains continued to be recovered from the ashes.

Suddenly, we were vulnerable. Not just to disease, tornadoes, accidents, or criminals, but to the kinds of enemies that had always threatened others but never us.

Barack Obama remembers that after the second plane hit, he left the Chicago building that housed his state-Senate office. “I stood in the street and looked up at the Sears Tower, fearing it might be a target, too,” he told me in a recent email exchange, adding, “I remember rocking Sasha to sleep that night, wondering what kind of world our daughters were going to grow up in.” He continued, “With nearly 3,000 people killed in the places where we lived our daily lives, there was a feeling that our homeland was truly vulnerable for the first time.”

This is the story of the first 15 years of how we have dealt with that newfound fear—how we have confronted, sometimes heroically and sometimes irrationally, the

mechanics, the politics, and the psychic challenges of the September 12 era.

FROM OUR SEPTEMBER 2016 ISSUE



Try 2 FREE issues of *The Atlantic*

SUBSCRIBE

Have we succeeded in toughening up what overnight became known as “homeland security”? Absolutely. But not without a series of extravagant boondoggles along the way.

Are we safer? Yes, we’re safer from the kind of orchestrated attack that shocked us on that September morning. It’s harder for terrorists to get into the country, and harder for them to pull off something spectacular if they do. But we have not plugged some of the most threatening security gaps. Worse, as the Orlando massacre reminded us, the world has become more populated by those who want to exploit those gaps, including those living among us—and who, in the United States, can easily obtain military-grade weapons. They are not deterred by the prospect of their own death, and they are happy to commit acts less ambitious than those of 9/11. That makes their attacks much harder to detect in advance. Our defenses are far stronger, but what we have to defend against has outpaced our progress.

Have we adjusted, politically and emotionally, so that we can make rational decisions as a government and as a people to deal with the ongoing threat? Not yet. In a bitterly divided democracy, where attention spans are short and civic engagement is low and the potential for oversimplification and governing-by-headlines is high, that is hardly a surprise.

But in those first hours after the planes hit their targets, we did answer the call—which required an almost complete turnaround of America’s mind-set and produced just as stunning a turnaround in our security posture.

Part I: The Good News

On September 10, 2001, then–Attorney General John Ashcroft rejected an FBI request to increase anti-terrorism personnel for the coming fiscal year beyond a fraction of the bureau’s overall staff. The next morning, Ashcroft headed to Milwaukee to read to schoolchildren while his boss, President George W. Bush, was doing the same at an elementary school in Sarasota, Florida.



America's struggle to cope with the relentless threats of the post-9/11 world
[Read more](#)

Also on September 10, FBI officials declared at a congressional briefing that the most imminent domestic terrorism threat was from animal-rights activists. Fifteen years later, the Justice Department has a national-security division, set up in 2006, that has consolidated and fortified all the department’s counterespionage and counterterrorism litigation and related legal-policy decisions. The overall FBI budget has nearly tripled since 2001, and its mission of investigating and prosecuting federal crimes that have already happened has been expanded to stopping terrorists before they strike. Most of the new resources—for intelligence analysts, technology upgrades, and additional agents—have been directed at prevention. “About half” of all agents are now assigned to national security, FBI Director James Comey told me, up from “maybe a quarter before the attacks.”

Connecting the Dots

On September 10, 2001, the Federal Aviation Administration, which was responsible for air-travel security, had a watch list of 12 people, even though the FBI and the CIA had identified hundreds more in their databases. A proposal to expand the FAA list to include those additional names had been sitting for months in the inbox of an FAA security official. In reporting for a book about the nation’s recovery efforts in the first year after 9/11, *After: How America Confronted the September 12 Era* (2003), I discovered that two of the hijackers had been on that

expanded list. Distribution of their names to the airlines had been delayed because the FBI and the FAA had not resolved which organization's letterhead should be attached to the memo bearing the new list.

On the day the World Trade Center fell and the Pentagon was left smoldering, the CIA knew that two suspected terrorists whom it was tracking around the world—and who ended up on the 9/11 planes—had come to the U.S. months earlier. But the agency never told the FBI. When this came to light, the September 12-era phrase *failure to connect the dots* was born.

Today, all U.S. security agencies share the same watch lists and threat databases, which are constantly updated. They share intelligence tips with one another (though sometimes still grudgingly), and federal officials even sit on task forces with their local counterparts. With some lingering exceptions, we do connect the dots.

Safety in the Air

On September 11, the airlines themselves were responsible for airport-security lines. They employed 16,000 poorly trained, low-wage private screeners, who operated under guidelines, approved by the FAA, that allowed the kind of box cutters and knives (up to four inches long) that the hijackers used. The airlines had lobbied the FAA for these and other accommodations to keep costs down and the security lines moving.

Today, there are 46,000 screeners, almost all federal employees, trained by the Transportation Security Administration. Although management failures have produced security gaps in fast-moving lines, followed by—especially this spring and summer—long wait times resulting from efforts to plug those gaps, the screening process is undeniably tighter than it was on the morning of September 11. And cockpit doors have been fortified to block anyone who slips past the screeners, making a repeat of the 9/11 plot to commandeer planes and turn them into missiles hard to imagine.

In the 1970s, hundreds of federal air marshals—undercover cops in the air—were deployed on American planes to thwart hijackings to Cuba. By 2001, the number of marshals had been reduced to 33—negligible coverage for the more than 20,000 flights leaving 440 airports in America every day. Within a month of 9/11, an emergency program had recruited 600 new marshals, and by 2005 approximately 5,000 were on planes. (The actual number is classified.)

Securing the Ports

When Kevin McCabe, the chief inspector of the U.S. Customs contraband team at the giant Elizabeth, New Jersey, freight port, looked across the water at the World Trade Center in Lower Manhattan and saw the second plane hit, he knew his country was under assault.

McCabe stared out his office window at the pier below, loaded with more than 7,000 cargo containers that had arrived from all over the world, and began what was probably America's first exercise in post-9/11 profiling. He directed his 70 inspectors to move every container that had arrived from the Middle East or North Africa—about 600 of them—to a far-off section of the pier. They then began the days-long process of X-raying and, if anything seemed untoward, hand-searching all 600.

 **A U.S. Army sergeant patrols the main concourse of Grand Central Terminal, July 4, 2016. (Greg Kahn)**

The X-rays and searches, however, had always been geared to looking for smuggled drugs. The inspectors were great at finding cocaine hidden in limes from Ecuador. But they had little training in looking for bombs—and little equipment for detecting material that could be used for a radiation-laced “dirty bomb.”

Fifteen years later, every American port screens cargo using billions of dollars’ worth of technology, including radiation detectors. Containers that register high on a threat matrix (based on information sent in advance about the content and its shippers) are singled out for additional screening; many containers are screened in foreign ports by U.S. Customs inspectors before they set sail.

The system is far from airtight. But the port inspectors have come a long way from McCabe’s panicked game of musical containers.

Preparing for a Biological Attack

A week after the attacks, America was again caught flat-footed, when envelopes containing deadly anthrax were sent to several media outlets and two U.S. Senate offices, ultimately killing five people and hospitalizing 17. When Tom Ridge, the Pennsylvania governor, whom President Bush had just recruited to become the White House homeland-security adviser, convened his first meeting about anthrax in the Roosevelt Room, across from the Oval Office, he was stunned by the cluelessness of those assembled at the table. There was no playbook. No list of medical experts to call. No emergency supply of antidotes and no plan to produce one.

Today, a collection of federal agencies—so many that, if anything, there is bureaucratic overlap—has playbooks for a variety of biological and chemical outbreaks, and billions have been spent to stockpile antidotes.

Part II: The Spirit of September 12

Beginning September 12, 2001, crash efforts were the order of the day.

Reconstituting the air-marshals program.

Doubling the number of Border Patrol agents.

A Victim Compensation Fund was conceived of and passed by Congress in 10 days and became the nation's single greatest act of tort reform. To the dismay of many trial lawyers, it allowed victims' families to seek millions each in uncontested claims directly from the federal Treasury (and also bailed out the airlines).

The TSA was legislated and launched within months, led by a fresh group of recruits from the private sector. They held their first meetings standing in an empty room in the Department of Transportation's headquarters, clutching laptops—until someone gave up on the glacial government procurement system and went to a local Staples and ordered chairs and desks with his own credit card.

Tom Ridge was emblematic of the September 12 mind-set. He'd been the governor of Pennsylvania for nearly seven years, and loved his work. But he took the job heading homeland-security efforts within hours, on September 19, not knowing where he would live or what his salary would be. This same spirit moved members of Congress to pass piles of bipartisan legislation and assemble on the Capitol steps the night of the attacks, holding hands and singing "God Bless America."

Video: The Inevitability of Dirty Bombs



0:00 / 4:00



The terror threat that no one is talking about

OF COURSE, THAT HAS CHANGED. The initial September 12 spirit was like a rush of adrenaline. Much of what Americans in and out of government did was extraordinary; in hours worked, helping hands extended, immediate problems solved, they stretched beyond what they might have expected of themselves.

Then the rush subsided. When the headlines—the adrenaline that fuels Washington—died down, Beltway norms returned. Contractors, consultants, academics, and bureaucrats swarmed in to co-opt the new big thing, while the politicians retreated to their respective corners.

In April 2002, working as a reporter, I watched as a spirited band of new recruits got the TSA up and running at its first airport, in Baltimore. They timed passenger throughput, and high-fived each other when it stayed below four minutes per person. When the sun glared through a glass wall, killing the view of a carry-on-bag X-ray machine, someone found a piece of cardboard to shade it. More high fives.

When I visited TSA headquarters five years later to discuss a business I was starting that would expedite prescreened passengers through the security lines,

administrators and other back-office employees—who by now numbered about 5,000, in addition to the 44,000 screeners working in airports—had their own building, near the Pentagon. As I rode the elevator, two people with TSA ID badges got on. One grouched to the other that his parking-space assignment was unfair.

“Even I think the pendulum has swung way too far” in the direction of overspending and bureaucracy, says Richard Clarke, the anti-terror chief on President Bush’s National Security Council, who had been derided for being the guy in the White House most obsessed with the threat of an al-Qaeda attack.

“Beginning almost the morning after, the consultants and contractors came out of the woodwork.”

Billions of dollars awaited contractors who promised infallible new technology: bio-threat and radiation detectors in towers to catch border-jumpers, upgraded Coast Guard cutters, biometric identification cards, \$1 million baggage-screening machines, new data-collection software.

Billions more would go to cities and towns savvy enough to slap a homeland-security label on grant proposals.

A burgeoning industry of homeland-security conferences and trade shows sprang up.

Across the country, colleges and universities went after research grants aimed at everything from how to make office windows blast-proof to how to secure international shipping channels. Academic institutions began offering degrees in homeland security. I counted 308 such programs when I scanned the web a few weeks ago.

“Sure, we’re safer than we were 15 years ago,” says one senior auditor at the Government Accountability Office (GAO), whose 3,000 auditors independently monitor federal agencies. “But we’ve spent hundreds of billions since 9/11. The question is how much of that was wasted and how much should have been used on other programs to address other security gaps.”

Bioterror and "Failures of Imagination"

Here are excerpts from an eye-opening report highlighting one of those continuing gaps, which I bet you never heard about, even though it was issued less than a year ago:

Nine weeks ago, terrorists unleashed insidious biological attacks on our Nation's Capitol during our Independence Day celebrations. The infectious agent they used ultimately led to the deaths of 6,053 Americans ...

We discovered later that other attacks had already begun elsewhere in the Nation, using methods we have yet to identify that spread the disease among livestock in rural communities.

The report then offered a stinging indictment of America's security apparatus:

The terrorists were successful because the government—including Congress—failed. They took advantage of our failure to achieve early environmental detection of the agent, failure to quickly recognize its occurrence in livestock, failure to rapidly diagnose the disease caused in sick patients, failure to consistently fund public health and health care preparedness, failure to establish sufficient medical countermeasure stockpiles, failure to make sure that non-traditional partners communicate. Ultimately, they took advantage of our failure to make biodefense a top national priority.

Sadly, much as the 9/11 Commission observed in its analysis of the attacks of 2001, the attacks of 2016 occurred because of another “failure of imagination.”

The report was written by an all-star bipartisan panel consisting of, among others, Tom Ridge, the founding secretary of the Department of Homeland Security; Joe Lieberman, the former chair of the Senate Homeland Security Committee; Donna Shalala, who served as the secretary of health and human services under Bill

Clinton; and Tom Daschle, the Democratic former Senate majority leader. They were organized by Lewis “Scooter” Libby, who now works at the Hudson Institute, a conservative think tank. As Vice President Dick Cheney’s national-security adviser, Libby led the country’s bioterrorism-defense initiatives following 9/11 and the anthrax attacks.

No, the attack described in the report didn’t actually happen. Rather, the authors introduced the scenario as something that *could* happen, because, they wrote, “the threat is real and growing” and “carries with it the possibility of millions of fatalities and billions of dollars in economic losses.” It was meant to be a “wake-up call” to get the nation’s attention, Ridge told me.

It didn’t work. The rest of the report drew on dozens of experts’ testimony and reams of data to present the case for renewed attention and national leadership to address the threat of bioterrorism, which Libby says is “still the most likely game-changing terrorist attack.” Yet the report received scant news coverage when it was issued on October 28.

The Obama administration had the same nonreaction. The panel’s primary recommendation—to put one senior person in charge of consolidating the hodgepodge of agencies that have some role in biodefense—has never been acted on. “I read the report, and I respect it,” Jeh Johnson, the Obama administration’s current secretary of homeland security, told me. “But it’s a lot like everything else I deal with. We have to make choices every day about risk and priorities.”

What a difference 15 years makes. The bioterror threat hasn’t receded; if anything, as the panel pointed out, advances in science and technology have made it easier to launch these kinds of weapons. But the nation’s attention has receded—which is emblematic of the roller-coaster way our democracy and its leaders deal with risks. As suggested by the report’s rhetoric about “failures of imagination,” our imagination is limited to the day’s headlines. Policy makers fight the war that made those headlines, not the war that might come next.

A week before the 9/11 attacks, three *New York Times* reporters—Judith Miller, William J. Broad, and Stephen Engelberg—published an article in *The Times* adapted from their book, *Germes*, a vivid account of the danger of bioterrorism that would be published the following month. After the Twin Towers fell and the anthrax envelopes were delivered, *Germes* shot to the top of best-seller lists and the media were filled with reports about how a successful biological attack could kill as many people as a nuclear weapon—yet would be far easier to pull off, a point that had been made earlier, by the 1999–2001 commission led by former Senators Gary Hart and Warren Rudman, whose pre-9/11 warnings about a terrorist attack on the U.S. were widely ignored.

**The inspectors' specialty was finding cocaine hidden in
limes from Ecuador. They had little training in looking
for bombs.**

Immediately after the anthrax attacks in September 2001, Libby got Cheney and the rest of the Bush administration behind an urgent biodefense drive. Within months, during which there were several false alarms signaling apparent follow-on germ attacks (including one that officials feared had penetrated the White House), what would become a program costing hundreds of millions was launched to buy dozens of BioWatch detectors. These were deployed at pedestrian gathering places in 20 major cities to collect air samples. By 2005, 36 metropolitan areas were covered.

The instinct to do something, anything, about the threat was understandable. But collecting and analyzing BioWatch air samples could take up to 36 hours. By then, of course, an aerosolized attack could have infected thousands of victims who would have long since dispersed. Besides, samples of only six possible pathogens

were even theoretically detectable, and that was only if the offending germs were sprayed close to the detectors.

Worse, it wasn't clear that even those six pathogens would be detected at any distance. According to GAO reports about BioWatch and a study by the National Academy of Science, the devices had never been tested in real-world conditions, because officials hadn't determined how to avoid the obvious risks during the testing process. The sensors deployed indoors (at places like Grand Central Terminal) seemingly had a better chance of working than those scattered outside along busy streets. But no one knew for sure whether any of them worked.

A new BioWatch program was launched in 2003 to develop systems that could cut down the analysis process to six hours and broaden the range of threats that could be detected. The effort lasted 11 years and ate up another \$200 million in fees to Beltway contractors. But it was canceled in 2014 because the new devices didn't work.

Meantime, the original sensors are still deployed. Whether they work is still not known; many experts doubt they do unless the aerosol is released in intimate proximity. The continuing 36-hour sample-collection process and related maintenance cost \$80 million a year—more than \$1 billion over the past 15 years.

As of the end of 2014, the BioWatch sensors had produced a total of 149 alarms—none of which, according to a 2015 GAO report, “was linked to an attack or to a public health threat.” In fact, BioWatch is considered such a dud that local officials routinely ignore any alarms that federal homeland-security officials pass along from it.

“We knew it was a stopgap, but we felt we had to put something out there” at the time, says Ridge, who was the homeland-security secretary until the beginning of 2005. “But 13 years, and nothing better? Come on!”

 **Tom Ridge, America's first secretary of homeland security, in his office in Washington, D.C., June 27, 2016 (Greg Kahn)**

This past February, when a House homeland-security subcommittee held a hearing on BioWatch, senior DHS officials assured their inquisitors that they were working

on the problem. “We seem to be having the same hearings over and over again,” Bennie Thompson, a longtime Democratic subcommittee member, complained.

The subcommittee’s then-chair, Martha McSally, a Republican freshman from Arizona and a former Air Force fighter pilot, seemed more upbeat, until she noted that industry vendors had told her they’d responded to DHS requests for information about possible new versions of the technology two years earlier but never heard back. Reginald Brothers, the Homeland Security Department’s undersecretary for science and technology, replied that he was now sending out still more such requests. Testifying in a near-empty committee room that would have been filled with bioterror-obsessed media 15 years earlier, the undersecretary said his team was engaged in an “exploratory process” and hoped to have a fix in place in “three to eight years.”

“This kind of stuff just drives you crazy. It’s all so slow and bureaucratic,” McSally told me. “We rolled something out in a panic after 9/11 and then it lingered in a substandard place because attention shifted.”

When I asked Jeh Johnson about his deputy’s apparent acceptance of a process whereby exchanges of information with the private sector stretch out over years and whereby a fix to an urgent problem is still three to eight years off, he sighed in what seemed to be exasperation, then offered this: “I can think of a number of instances where the best technology is a ways off.”

“When germs were sexy right after 9/11, they focused on it,” says Judith Miller, one of the co-authors of *Germs*. “But until someone engineers one of these pathogens and releases it, we’re not likely to do anything more.”

“Jack Bauer Syndrome”

The story of BioWatch’s exercise in hope over reality illustrates what one GAO auditor calls “Jack Bauer Syndrome,” referring to the counterterrorism agent who was featured in 24, the hit TV series.

“If you’re shocked and scared and you know there’s a threat out there, you’ll do anything, spend anything, to deal with it,” the auditor explained, “even if what you spend it on hasn’t been tested and you haven’t even set any standards to evaluate it.”

Chip Fulghum, the Department of Homeland Security’s chief financial officer, who took the job in 2013 and says he considers himself part of a “cleanup operation,” puts it this way: “Right after 9/11, the spigot got turned on and a fire hose of money poured out. Much of it was badly monitored and much of it was for stuff that just didn’t work.”

Multiple programs—salivated over by Beltway contractors, who formed “capture teams” to reel in business—were launched with exuberant announcements, after which they quietly tailspinned into implementation delays, revised promises, and finally failure.

**“We rolled something out in a panic after 9/11 and then it
lingered in a substandard place because attention
shifted,” Martha McSally says.**

Two billion dollars was doled out to improve the TSA’s screening of checked bags for bombs, but the new equipment yielded no discernible improvement.

RELATED STORY



[The \\$47 Billion Network That’s Already Obsolete](#)

Another \$1 billion was wasted on a network of motion sensors and camera towers across just a fraction of the U.S. border with Mexico as the first step in what was to be a \$5 billion program. When the government awarded the coveted contract to

Boeing in 2006 (to replace a failed \$2.5 billion program started in 2004), President Bush heralded it as “the most technologically advanced border project ever.” Once deployed, however, the system’s sensors set off alarms when all varieties of wildlife moved around, and its cameras swayed in the wind and failed to provide visibility in areas where the land wasn’t level. The program was finally euthanized in 2011, after which an Israeli firm was brought in to provide a system that apparently works.

Similarly, a \$2.5 billion plan to replace drive-through radiation detectors at border crossings with a new model that would cut the high false-alarm rate was killed in 2011 after \$230 million in prototype tests showed no improvement.

A long-running contract awarded to Northrop Grumman and Lockheed Martin to build new Coast Guard cutters has so far come in \$1 billion above its \$4.7 billion budget and four years late.

And a \$400 million program (also feasted on mostly by Lockheed Martin) to distribute 3.5 million tamperproof biometric ID cards to truck drivers hauling hazardous material and to workers at seaports and airports was completed five years behind schedule, in 2011. Worse, the ID-card readers have never worked and are not being used, making the high-tech credentials no more secure than a library card.

The granddaddy of all the misbegotten big ideas may be something called FirstNet, a project set up to provide a telecommunications system exclusively for firefighters, police officers, and other first responders [that would cost as much as \\$47 billion](#).

“Attack 2” Versus a Flaming Bagel

Clarke, the former White House anti-terror chief, has a weekend house in Rappahannock County, Virginia (population 7,400). He says that one Sunday morning a few years after the 9/11 attacks, he burned a bagel in his toaster and his smoke alarm went off. “This monster fire truck with four volunteer firemen—two teenagers and two guys my age—arrived,” Clarke recalls. “They could barely drive the thing. It had a logo on it calling it ‘Attack 2.’” Clarke was stunned to find out

that the truck had been paid for in part by a \$160,000 federal homeland-security grant.*

“Want to see how your homeland-security money was spent?” a longtime anti-terror official who was one of Tom Ridge’s senior aides asked me. “Go to your local Fourth of July parade anywhere in small-town America and you’ll see a logo on a spiffed-up fire truck or armored police truck saying we paid for it.”

The largesse has hardly been limited to souped-up emergency vehicles. Across the country, small towns have loaded up on everything from a “latrine on wheels” in Fort Worth, to fish tanks in Seguin, Texas (presumably to help counterterrorism cops relax?), to unspecified equipment in American Samoa. In all, more than \$40 billion has been spent on homeland-security grants since 9/11.

 **U.S. Representative Martha McSally of Arizona, the chair of a House subcommittee on homeland security, at her office in the Longworth building, Washington, D.C., July 6, 2016 (Greg Kahn)**

Everything in the grant applications was linked to terror, an exercise in which the grant writers suffered no failures of imagination. A Senate report documenting this spending found that one law-enforcement website offered “a how-to guide, *Tapping Into Federal Funds*, advising public safety officials to amplify the frightening ‘what ifs’ in their request for funds by pointing out ‘the worst case scenario’ ... that the project for which you’re seeking funds would help.”

The arrival of Attack 2 to extinguish Clarke’s bagel was proof that homeland security had morphed from an emergency mission into politics as usual. When asked during a 2004 Senate hearing what kind of formula governed decisions about who received grants, Tom Ridge, himself a former congressman, replied in a burst of candor that he was looking for something that gets “218 votes in the House or 51 votes in the Senate.” This explains why Congress mandated that each of the 56 states and territories had to receive some grant money, regardless of actual risk of terrorism.

Today, the grants continue, though at a reduced rate, and they are mostly restricted to high-risk metropolitan areas.

Which is the other side of the story.

Money Well Spent

The flow of federal funds to major cities has plugged innumerable security gaps.

In New York City, federal grants enabled newly elected Mayor Michael Bloomberg and his police commissioner, Raymond Kelly, to set up a 1,000-person Counterterrorism Bureau that includes specially armed quick-response units and intelligence officers assigned overseas.

On September 12, 2001, the train tunnels under New York’s rivers could have been breached by a bomb small enough to fit in a backpack. Thousands could have been drowned. The most vulnerable were PATH trains running under the Hudson River to

New Jersey. Hundreds of millions of dollars were quietly allocated to reinforce the tunnels' roofs.

More federal money went to reinforcing subway tunnels, installing cameras to detect intruders, and assigning undercover officers to ride the trains.

Money from Washington helped pay for the hardening of the Madison Square Garden–Penn Station complex, a venue that had been easy prey for even a small car bomb and that—because it is a high-profile, crowded hub sitting atop crucial subway junctions and Amtrak's Northeast Corridor rail lines—was feared to be a prime terrorist target.

On the Upper West Side, an exposed bit of a pipeline running natural gas up the East Coast was encased in a protective shed, as was a vulnerable water main in the Bronx that could have flooded much of that borough.

RELATED STORY



['We Will Defend Our Nation': An interview with Barack Obama on homeland security](#)

Federal money helped pay for a team of consultants to work with Kelly's Counterterrorism Bureau to produce a smartly written manual called "Engineering Security." Now widely used across the country, it provides those responsible for the security of office buildings and other facilities guidance on everything from gauging the blast resistance of different grades of glass to determining a venue's overall risk profile.

Washington also paid for cops to be posted at key targets. At the Brooklyn Bridge, according to Kelly, these officers staved off a plot to cut its cables—which intelligence officials learned about when questioning Khalid Sheik Mohammed, al-Qaeda's 9/11 mastermind.

Overall, anti-terror money sent from Washington to New York has exceeded \$6 billion.

The federal government made similar investments in other cities and other high-profile venues across the country. Joint Terrorism Task Forces—which had previously consisted of small groups of FBI agents, representatives of other federal law-enforcement agencies, and a few local police officers—were beefed up with funding from Washington. The number of detectives and intelligence analysts on Ray Kelly’s task force in New York went from 17 to 120.

In 2001, there were 35 Joint Terrorism Task Forces around the country; today, there are 104. The federal government has also funded broader groups of law-enforcement and emergency-response agencies, called fusion centers.

The feds have sponsored drills and other exercises to help state and local police departments, and other first responders, rehearse how they would work together in an emergency. One full-scale, 24-hour exercise in Massachusetts, six months before the April 15, 2013, bombing of the Boston Marathon, is credited with helping officials do such a good job of stationing medical personnel at the site before the event began and mapping out how mass casualties would be distributed to the city’s multiple trauma centers that, amazingly, none of even the most grievously injured among the 264 victims was added to the death toll of the three who died immediately at the scene.

Part III: Washington’s Most Maligned Agency

By my calculation, over the past 15 years, the American government has spent \$100 billion to \$150 billion on failed or unworthy homeland-security programs and on acquiring and maintaining equipment that hasn’t worked. However, as with the equipment procured for port inspections, launching the TSA, and grants for protecting New York’s subway tunnels and running emergency drills in Boston, much more than that was well spent.

The same mixed verdict applies to the agency created to dole out that money and manage the programs. President Bush’s decision to combine 22 far-flung government agencies into the Department of Homeland Security belatedly

followed a primary recommendation of the Hart-Rudman commission, whose warning, in three reports starting in 1999 and culminating on January 31, 2001, about the need for the government to prepare for terrorist attacks had been largely ignored. The details of the reorganization are still being debated. Should the FBI have been left out? Should the Secret Service have been included? But combining agencies such as Border Patrol, Customs, the new TSA, and the Federal Emergency Management Agency into one department responsible for putting the people and systems in place to defend against or recover from an attack made sense, as did enabling the still-separate FBI to gather intelligence in order to stop the people planning attacks or track them down after an attack occurred.

Nonetheless, the result, especially at first, was management disarray and ineffectiveness that could fill a textbook on bureaucratic dysfunction.

DHS—which has had seven undersecretaries or acting undersecretaries for management—has perennially been on the GAO’s list of agencies whose overall management is considered “at risk.” From the beginning, the agencies thrown into the new superagency fought to keep their turf, often calling on congressional allies to help. “At one meeting early on, I mumbled something about why should the Coast Guard and Customs each have their own helicopters and planes,” Tom Ridge recalls. “Why couldn’t they combine to purchase the same stuff? Within a few days, we had calls from Capitol Hill warning us not to mess with the Coast Guard’s or Customs’ procurements.” (The two agencies still have their own air forces.)

Ridge was preoccupied during his tenure with organizing the new agency and launching urgent programs, like the BioWatch detectors and the posting of U.S. Customs inspectors overseas. His successor, Michael Chertoff, a former federal appeals judge and head of the U.S. Justice Department’s Criminal Division, prioritized tighter management, but ended up overwhelmed during most of his tenure by his department’s failures in the aftermath of Hurricane Katrina. Chertoff, who declined repeated requests to be interviewed, was succeeded during President Obama’s first term by Janet Napolitano, who resigned as governor of Arizona to head the department. Napolitano focused, she told me, on rebuilding FEMA

following the Katrina disaster, border security, and the (unsuccessful) effort to pass a broad immigration-reform bill.

**The border-control system's sensors set off alarms when
wildlife moved around. The program was finally euthanized
in 2011.**

Only Jeh Johnson, who succeeded Napolitano when she left to take over the University of California system in late 2013, seems to have made forging a cohesive organization—he calls it “unity of effort”—a priority.

Johnson, who turns 59 on September 11, was the first African American to make partner at Paul, Weiss, Rifkind, Wharton & Garrison, a New York law firm that has long been a home for prominent Democrats who rotate in and out of government. A former general counsel for the Defense Department, Johnson seems to have become a smart, tough manager. He has made significant progress in rationalizing DHS, which today is a \$64.9-billion-a-year colossus with 240,000 employees. But the challenges of fusing so many long-standing independent bureaucracies remain, even 14 years after they were first thrown together.

Dealing with these multiple agencies is further complicated by the fact that DHS's senior executives and staff are spread among 120 offices, scattered, wherever space has been available, throughout Virginia, Maryland, and the District of Columbia. Most work far from Johnson's office, a shabby, converted naval facility in Northwest D.C. that is itself far from downtown Washington. (After many false starts, a closer-in, massive \$600 million headquarters seems likely to be built within the next two or three years.)

The Office of Personnel Management's latest annual survey of employee morale across all government agencies ranks DHS in the bottom tier across multiple


measures of employee satisfaction and sense of mission. In a category called “intrinsic work experience,” DHS somehow scored below the Federal Elections Commission, an agency so famously paralyzed by partisan deadlock that its mission has basically been put on hold.

“I really care about that survey, and we’re going to improve those numbers,” Johnson told me. “But it’s going to take time.”

An approachable boss who has made a habit of mingling with his troops wherever he goes, Johnson seems well suited to the challenge. At a town-hall meeting for DHS employees in New York, I watched him connect with those who asked questions, inquiring about their families and then demonstrating that he was immersed in the issues they cared about. Last March, Johnson was a big hit at the Baltimore-Washington International airport when he played undercover boss, acting as a TSA screener.

“I wasn’t planning to be a manager when I came into this job,” Johnson said. “But during my [Senate] confirmation-oversight process, I kept hearing ‘management reform, management reform,’ so this is something I’ve had to focus on.”

Although the GAO recently reported that DHS has made significant progress in tightening management, Johnson still has work to do, starting with customer service. In June, a friend tried to call Customs and Border Protection with a complaint about a Global Entry card that he should have been able to use when entering the United States after an international flight. The line was constantly busy, so he tried the agency’s email complaint system, only to receive a reply telling him that the response time for emails like his was “16–20 business weeks.” I followed up and called three different DHS customer-service lines. No one ever picked up the phone.

 **Jeh Johnson, the current secretary of homeland security, who has made improving the dismal morale of his department a priority, at DHS's New York office in One World Trade Center, June 20, 2016 (Greg Kahn)**

Last winter, a House subcommittee hearing about a DHS human-resources IT program produced another installment of a C-SPAN drama that has played out in dozens of episodes since the agency was put together: indignant inquisitors lacerating their witness. Noting that the IT program had so far cost \$180 million over 13 years without yet being operational—and that there is no set schedule for when it would be—Scott Perry, a Pennsylvania Republican, told Chip Fulghum,

DHS's chief financial officer, that the program was the "poster child for inept management."

Congressional Malpractice

As Perry's scolding of Fulghum demonstrates, members of Congress in both parties have never been shy about criticizing, even mocking, the Department of Homeland Security for mismanagement and low staff morale. But the longest-running failure of management when it comes to homeland security—a failure that is deliberate, self-centered, and easy to fix—has to do with Congress itself.

When Congress voted in 2002 to consolidate 22 federal agencies into a unified DHS, each of those agencies and their dozens of subunits was overseen by different congressional committees and subcommittees. "We figured congressional leaders would reorganize things," says Ridge, referring to how, after the departments of the Army, Navy, and Air Force were put into the new Defense Department, congressional oversight was consolidated accordingly.

That never happened. "There is no committee chairman or subcommittee chairman or ranking member who will give up jurisdiction over something that they had jurisdiction over, especially something as sexy as homeland security," Martha McSally, the House subcommittee chair, told me. Thus, four House and Senate transportation subcommittees oversee the TSA and the Coast Guard, but subcommittees of the House and Senate homeland-security committees oversee them too. In all, 119 congressional committees or subcommittees assert some kind of jurisdiction over DHS.

Those committees and subcommittees held 300 hearings in 2011 and 2012 alone, according to a tally compiled by DHS. Each hearing required DHS secretaries, undersecretaries, assistant secretaries, or agency heads to sit for hours, listening to the members read ponderous opening speeches and then responding to questions. It adds up to one or more senior DHS officials sitting through these hearings about

three times a week. And that's not counting the many more informal briefings conducted for members of Congress.

"It's outrageous," says Napolitano. "You get all those directions and priorities from all those committees and subcommittees. It's a huge burden and a huge waste of time."

When then-Speaker John Boehner was asked during a December 2014 press conference why oversight hadn't been consolidated under the homeland-security committees, he chuckled and said, "I've been working on this for about six years ... It should have been done."

I could find no member of Congress or congressional staffer willing to defend the current setup. Rather, unlike any other issue when it comes to terrorism—where urgency and indignation at even the slightest failing is the order of the day on Capitol Hill—everyone I talked with seemed to accept their own bipartisan failure to act as an immovable fact of life.

The Duct-Tape Dilemma

Some morale problems at DHS may have less to do with management and congressional harassment and more to do with the nature of DHS's mission. There are few noticeable victories—but multiple opportunities for failure, embarrassment, and ridicule.

"The FBI are the stars and the DHS people basically are seen as the garbagemen," Richard Clarke told me. While the FBI, he explains, does high-profile detective work, DHS mostly screens people and things at airports and borders, reviews claims for cleanup grants after disasters, and does the unsung work of advising the private sector on how to protect its infrastructure. Even DHS's arguably most glamorous agency, the Secret Service, makes headlines only when it fails.

"In law enforcement," says Johnson, who is a former federal prosecutor, "you get a big takedown and you get a big press conference." You get headlines like "Eight

Charged in Check-Kiting Mob.” But the nature of homeland security “is different. We’re on defense.”

Although DHS mostly makes the news when it fails, it also gets attention when it becomes the butt of comedy monologues about mindless bureaucracy.

Early on, the jokes had to do with color codes and duct tape. Both illustrate the no-win proposition of having a government agency try to deal with the changing impulses of the September 12 era.

The much-ridiculed color codes—public pronouncements that the country was at a green, blue, yellow, orange, or red state of alert—came about because Ridge insisted that federal officials should share threat information with the local police agencies who would be on the front lines. But the information the locals got was leaked, spurring outcries that the public deserved to know at least something about potential threats.

The resulting color scheme, announced in 2002, was derided as so vague as to be meaningless. But it was seen as better than the alternatives of saying nothing or telling everyone, including the bad guys, specifically what the government knew. Ten years after the attacks, the color advisories were abandoned in favor of equally vague but wordy “bulletins” that are infrequently updated on the DHS website, where they are largely ignored but are no longer a source of derision.

Duct tape was about a more important, if equally ridiculed, initiative. In the aftermath of the anthrax crisis, amid growing fears of bioterror attacks, Ridge’s office urged citizens to prepare emergency “ready” kits. One of the suggested ingredients—in addition to flashlights, a portable radio, water bottles, and nonperishable food—was duct tape, which could be used along with plastic sheeting to seal doors and windows so that people could safely “shelter in place.”

This was, and remains, a prudent security precaution. But Ridge and his team were almost immediately lampooned, perhaps because joking about a possible disaster relieved nerves. Of course, if Ridge had discarded experts’ recommendation that he

tout duct tape because it could protect people during a bio attack and then an attack had occurred, he would have been denounced for his failure of imagination.

The Agency That's Always Wrong

DHS's most visible unit is the Transportation Security Administration, which has more daily interactions with more Americans than any other federal agency. Those encounters are inherently a source of public cynicism: They're inconvenient, and to many they seem an exercise in bureaucratic rigidity.

In June 2015, news leaked that testers from the DHS Office of the Inspector General had been able to smuggle simulated weapons or explosives through checkpoints 67 out of 70 times at airports across the U.S. Johnson was so incensed that he removed the acting TSA administrator and replaced him with Peter Neffenger, a highly regarded Coast Guard vice admiral. Since taking over, Neffenger has completely redone the TSA training program and required all current staff members to be retrained to focus on the agency's primary mission—security.

December 23, 2015. TSA lines have gotten worse this year, and will likely not improve until 2017. (Saul Loeb / AFP / Getty)

“We were worried too much about throughput,” Neffenger told me. “We had to go back to basics.”

Neffenger said he is also determined to expand the PreCheck program. Launched in 2012, PreCheck provides expedited TSA clearance for the 3 million people (so far) who have agreed to be prescreened. Neffenger is determined to improve its marketing, open more-convenient enrollment centers, and give government officials who already have a security clearance automatic enrollment.

PreCheck is “the most popular thing I’ve ever done in public service,” Napolitano, the former DHS secretary who initiated the program, told me. But it will be popular only until a PreCheck member does something bad—which is bound to happen today or 10 years from today, because no security process is perfect. Making homeland-security decisions based on logical weighing of risks makes sense and avoids public frustration and ridicule—until something bad happens.

As those who have flown lately know, the problem of slow airport-security lines was exacerbated this spring and summer by record air-travel volume and by the fact that three years ago, the TSA began to trim its airport staff. The staff cuts came because letting up on its tight process, which ultimately allowed the inspector general’s testers to slip through with their simulated weapons and bombs, had given DHS the false sense that it could keep the lines moving while getting by with fewer people. Hiring and training to get back to staffing levels sufficient to cut the current wait times while maintaining security will take at least until the beginning of next year.

Costs Versus Benefits

In the immediate aftermath of 9/11, fewer people flew, because they feared more aviation attacks. However, once the TSA was operating, people resumed flying

instead of driving. According to a study done by the University of Michigan Transportation Research Institute, there were likely 1,018 more traffic fatalities in the three months following 9/11 than there would have been had people believed flying was safe. In other words, the reassurance provided by the establishment of the TSA arguably saved more than 300 lives a month.

Put differently, terrorists can kill 300 people a month by scaring us off airplanes—and that's in addition to the economic havoc that fear of flying produces.

All of which suggests that judging the TSA's efficacy—and the claims about the agency's bureaucratic bloat and its pointless "security theater"—is complicated.

Of course, the TSA gets no credit for those 300 lives a month. Turning that theoretical math into congratulatory high fives is a stretch. But other, more direct measures of homeland-security success are no easier to calculate.

"How many terrorist attacks has TSA thwarted? We're never going to know the true answer to that question," Jeh Johnson says. "I do know that last year TSA seized in carry-on luggage 2,500 guns—83 percent of which were loaded."

Just before Tom Coburn, a Republican senator from Oklahoma famous for being waste-averse, left office in 2015, he issued a 162-page report on DHS that attacked almost every aspect of the agency for wasting money while "not successfully executing any of its ... main missions."

Coburn's argument boiled down to a recitation of the obvious: American taxpayers have spent \$1 trillion since 9/11 (on DHS and on terror-related work at other

agencies), but Americans are still not safe from terrorist attacks. Which is like declaring that a health-care system doesn't work because people still get sick and die.

“People ask, ‘How many terrorist attacks has TSA thwarted?,’” Jeh Johnson said. “We’re never going to know the true answer to that question. I do know that last year TSA seized in carry-on luggage 2,500 guns—83 percent of which were loaded.”

Coburn's attempt at more-detailed cost-benefit analyses highlighted how complicated that exercise can be. One of his most intriguing critiques was directed at the Federal Air Marshal Service, which, he pointed out, was spending about \$800 million a year (equal to about 40 percent of the Secret Service budget and nearly 10 percent of the FBI's). That adds up to more than \$10 billion since the 9/11 attacks. Yet, Coburn wrote, “it is unclear to what extent the ... program is reducing risk to aviation security.”

Air marshals are supposed to prevent terrorist hijackings. There have been no hijackings. Why complain about that? Isn't that the best possible proof that the program works? How do we know how many hijackers were deterred by the well-publicized air-marshal buildup?

RELATED STORY



[Meet the People Who Protect America's Critical Infrastructure](#)

Then again, even for \$800 million a year, the air marshals can be on only a fraction of all flights—maybe about 5 percent, depending on the number of air marshals, which is classified. No marshal was on board either shoe bomber Richard Reid's plane or the one carrying underwear bomber Umar Farouk Abdulmutallab.

And what about the flights that air marshals *were* on? On the hundreds of thousands of flights carrying undercover air marshals since 9/11, not a single hijacker has been taken down. In fact, there have been more arrests *of* air marshals since 9/11

(for off-duty conduct such as drunk driving) than *by* air marshals for conduct in airports or on planes.

This is what makes any cost-benefit analysis so challenging. There have been no hijackings since 9/11—and the deterrent value of having even a small percentage of flights protected by marshals might account for that. Yet training thousands of men (and some women) for armed combat in the sky and then having them travel (mostly in first class, to be near the cockpit) on endless flights every day does seem to be overkill, especially when all cockpits have been fortified to prevent the kind of forced entry that precipitated the buildup of the marshal force.

That would seem to be a good argument for at least dropping the Federal Air Marshal Service down on the DHS priority list. Yet only in the past four years have any members of Congress even mildly urged cuts in its budget.

Part IV: Everything Is a Priority

At least in the case of the air marshals, there is a tactical argument for cutting the program: The fortifying of cockpit doors and the arming of thousands of pilots may have eliminated the threat that the marshal program was supposed to address. But no one in Washington seems willing to rank threats in terms of the relative risk they pose. Saying that something is less of a threat than something else is a political third rail. Everything is always a priority.

Kathryn Brinsfield, a former emergency-room doctor and administrator of EMS services in Boston, is the DHS assistant secretary running the agency's bioterror-prevention programs, including the BioWatch sensors that have been waiting 15 years for next-generation technology. Those are the upgrades that one of her colleagues told Congress he hoped to have within the next "three to eight years." When I asked her to discuss the obvious—that her bailiwick had lost the priority status it had in the months following the anthrax crisis—she gamely replied, "No, BioWatch is a major priority."

Jeh Johnson is only a bit more forthcoming: “We have to be concerned about all ranges of attacks,” he says. “I never categorize anything as low priority, but we have to look at what’s high risk and what’s less high risk and spend our time accordingly.”

The problem with ducking a real discussion about priorities is that it allows for decisions to get made ad hoc and out of the limelight, typically based more on what’s “hot” or on what’s a political priority than on what the evidence might dictate.

“Not Your Father’s Terrorism”

What’s hot today is the threat of lone wolves.

Even before the Orlando massacre, every government official or television pundit was talking about how lone wolves—terrorists acting on their own, or in small groups—are the major threat to homeland security, rather than the kind of centrally managed, patiently planned shock-and-awe attacks al-Qaeda launched on 9/11. Although the Brussels and Paris massacres were, in fact, organized by sizable cells emanating from ISIL in Syria, multiple one-off attacks have become relatively common, from the Boston Marathon to Orlando to San Bernardino to Fort Hood to Garland to Chattanooga.

It adds up to what Johnson calls “an entirely different global environment.”

“This is not your father’s terrorism,” says John Miller, a former CBS News senior correspondent who is now the deputy commissioner for intelligence and counterterrorism at the New York Police Department.

Miller has a newsman’s flair for describing the current situation pungently: “Al-Qaeda was an elite organization. They would turn people away,” he says. “ISIL does no screening; they do mass marketing ... Their attitude is ‘We don’t care if you’re a loser. And we don’t care about some apocalyptic event. Just go do your thing.’”

“You do not have to be smart to kill people this way,” Miller continues. “The fact that they’re morons is academic. Any moron could make the pressure-cooker bomb

those idiots used in Boston. The San Bernardino couple were idiots. If they had been directed by anyone, they'd have picked something a lot more crowded than the place where the guy worked. But ISIL latches on to people like that, telling them, 'It's okay to lash out at people you hate—in our name. It's okay that you're a loser. You can still have an impact. You can be a hero.' It's elixir for someone sitting in the glow of their laptop in their parents' basement."

Al-Qaeda's biggest failing was ego, Miller says. "Bin Laden thought of himself as a historic figure and that if he just blew something up that wasn't spectacular, he'd be just like the Palestinians. So they didn't go after malls or anything ordinary. ISIL is just the opposite."

**"Al-Qaeda was an elite organization. They would turn
people away. ISIL does no screening; they do mass
marketing," John Miller says. "Their attitude is 'We don't
care if you're a loser.'"**

So how do we guard against would-be killers sitting in their parents' basements?

Miller's team includes a crew of several dozen multilingual people sifting through websites and social media. "We have an easier time getting Arabic speakers than the FBI, because we don't have to put them through the security clearances that the bureau does," he says.

According to Miller, who served as the head of public affairs at the FBI from 2005 to 2009, 15 of the past 19 cases in which the FBI made arrests charging people with offenses such as planning to join ISIL stemmed from leads developed by his NYPD unit.

Carlos T. Fernandez, the FBI special agent in charge of the New York-based counterterrorism division, which runs the city's Joint Terrorism Task Force, told me he is "not sure" of Miller's count, and that "there were many [cases] where we were both working leads"—which, he added, "is really the point: The big change since 9/11 is how we work together."

Strengthening the FBI

Fernandez's New York operation is on three floors of an old office building overlooking the Meatpacking District in Lower Manhattan. The task force—whose major wins include the 2009 disruption of a bomb plot by a homegrown terrorist who had driven to Queens from Denver—now numbers some 400 federal, state, and local agents and investigators from the FBI, the NYPD, and all the metropolitan area's other law-enforcement agencies. That's a dramatic upgrade from when the unit was formed in 1980 with 10 FBI agents and 10 city detectives in response to threats from Croatian extremists and the Jewish Defense League. "Those were the good old days," says Fernandez, whose work as an agent on the task force in the months after 9/11 had him spending much of his time overseas chasing leads.

Divided into 17 squads, the office has jurisdiction not only over New York, but also over cases emanating out of Canada, western Europe, and Africa.


One squad chases down any and all tips from the public and refers those that seem credible to more-specialized units. Others hunt terrorists on the internet. Separate squads track ISIL and al-Qaeda. Has Fernandez's al-Qaeda team lost focus in the wake of ISIL's rise to prominence? "That's why we keep separate squads," Fernandez says, "so that they don't."

A weapons-of-mass-destruction unit looks for intelligence about dirty bombs and bioweapons, keeping tabs on, as Fernandez puts it, "the potential players in bio or nuclear who, if we got a tip, we would look at first."

"The threat information bubbles up from the units," Carl Ghattas, the head of the FBI's counterterrorism division at headquarters in Washington, told me. "It's a

triage process. You look at the patients in the emergency room and decide what needs your immediate attention or what needs some kind of longer-term initiative.” That raises the question of whether—as with DHS paying inadequate attention to bioterror vulnerabilities and, as we will see later, other federal agencies not doing enough to secure potential dirty-bomb material—the FBI’s triage process is allowing lower-profile, higher-impact threats to fester.

“You have to worry about all the marginal, stupid people that ISIL may motivate here,” James Comey, the FBI director, told me. “But there are still smart people waking up every day over there trying to kill us. We know ISIL is trying to develop chemical weapons. And you have to worry about that, too. Balancing those threats is a challenge today.”

 **Orlando police officers direct people away from the mass shooting at Pulse nightclub, June 12, 2016.**
(Phelan M. Ebenhack / AP)


Comey was a chief federal prosecutor in New York and then the deputy attorney general under George W. Bush until he left for the private sector in 2005. He

recalled that when he returned to government to run the bureau eight years later, “I felt like Rip Van Winkle.” His predecessor as FBI director, Robert Mueller, “had totally transformed the place.” The agency now has something like 3,000 intelligence analysts. “The way we use local police is probably the biggest single change. All in all, I think we really are a well-oiled anti-terror machine.”

However, Comey acknowledged that even in the brief time since he took over the bureau in 2013, the rise of lone wolves has changed the nature of the intelligence his agents have to try to collect. Detecting the plans of a lone wolf or a small group can’t be done by monitoring a known foreign terror cell. The bureau has tools to sift through social media to try to connect the dots—but the volume of the traffic and possible connections between all those dots make this a hit-or-miss proposition where only hindsight provides clarity. As of this writing, it’s unclear whether Omar Mateen, who massacred 49 people in Orlando, was in contact with anyone about his plans. True, certain clues suggested that Mateen might be a threat—but they were no clearer than the hints about the thousands of people like him who hit the FBI’s now-vigilant radar screens every week. No amount of resources, let alone compromises in constitutional rights, would make it possible for the bureau to detain or even surveil all these people.

“It’s hard,” said Comey, who spoke with me a few weeks before the Orlando massacre. “But I’m not ready to give up. We have to keep trying.”

The FBI had interrogated Mateen twice in the past, but never had cause to arrest him, or to keep him under constant surveillance. “We are looking for needles in a nationwide haystack,” Comey said at a press conference the day after the Orlando massacre. “But we’re also called upon to figure out which pieces of hay might someday become needles.”

 **FBI Director James Comey testifying at a House
Judiciary Committee hearing, March 1, 2016 (Spencer
Platt / Getty)**


In the aftermath of attacks like those in Orlando and San Bernardino, some critics charge that Comey and his people were not aggressive enough in monitoring or arresting the perpetrators of those attacks before they occurred. Others argue that the FBI has overstepped constitutional boundaries in its drive to find out what people might be planning, often by entrapping suspected terrorists into actually creating attack plans they might otherwise never have thought of.

“Since 9/11 the FBI has organized more jihadist terror plots in the United States than any other organization,” Peter Bergen, a longtime terrorism analyst, wrote in *United States of Jihad: Investigating America’s Homegrown Terrorists*, published early this year. Bergen cites several cases in which defendants have argued that while they might have expressed hostile thoughts to someone who ended up informing on them, the FBI stepped in and, through informants or undercover agents, created an attack plan for them, encouraged them to try to carry it out—and then arrested them when they proceeded with the attempted attack. In June, a *New York Times* report calculated that two-thirds of the bureau’s recent prosecutions of suspected ISIL supporters have involved undercover agents or informants engaged in aggressive sting operations.

“Think about it from our perspective,” Comey said when I asked about this.

“Suppose someone is overheard in a restaurant saying that he wants to blow something up. And someone tells us about it. What should we do? Don’t we need to find out if he was serious? Or was he drunk? The way to do that is to have someone engage him in an undercover way, not show up with a badge and say, ‘What are your thoughts in regard to terrorism?’”

“Plenty of times it’s a wing nut or some drunk, and we drop it,” he continued. In fact, an informant was assigned to sound out Mateen two years before the Orlando attack, after co-workers reported that he had allegedly made inflammatory comments about terrorists. But Mateen did not seem to be a threat.

 **John Miller, the NYPD’s deputy commissioner for intelligence and counterterrorism, January 7, 2015 (Drew Angerer / Getty)**

“People have had plenty of opportunities to try that [entrapment] defense, and it hasn’t worked,” Comey added. The FBI has charged approximately 90 individuals

with plotting a terrorist attack since 2013. So far, no entrapment defense has been successful.

Reaching the Kid in His Basement


Because finding such homegrown cases is difficult (not everyone blabs online, let alone in a restaurant, about their bad intentions), a new homeland-security acronym has come into vogue: CVE, or “countering violent extremism.” CVE is a program that aims to reach people who are so alienated or unstable that they may be susceptible to ISIL’s appeals.

Last September, President Obama authorized the creation of the \$50 million CVE program, to be run by a new Office for Community Partnerships at DHS. A big part of the effort has been making DHS’s “If you see something, say something” campaign more effective. Beginning as a billboard tagline created by the New York City transit system’s ad agency, the program has become an effective message enlisting the public to alert authorities if they notice something or someone that seems suspicious, such as a suitcase left unattended on a train. George Selim, the director of the Office for Community Partnerships, works with a staff of about 30—as well as with Jeh Johnson personally—to encourage leaders in Muslim communities to look for signs of trouble more subtle and further upstream than abandoned luggage, such as teenagers in schools or at mosques who appear disaffected.

“All the data from Boston to Garland to San Bernardino indicate that someone around them knew something but didn’t want to or know how to report it,” Selim, a former Justice Department community-relations liaison, told me.

Johnson, who has thrown himself into the CVE effort, says that when he goes into Muslim communities, he tells people that he understands profiling. His grandfather, he explains, was called to testify before the House Un-American Activities Committee, because “in 1949 any black man with a Ph.D. was suspected of being a Communist.” He says he tells Muslim community leaders that he “will be

your public champion, but that I have an ask, too, which is ‘Help us help you with homeland security. It’s your homeland too.’”

 **An SUV and evidence markers pertaining to the shooting by ISIL-inspired killers at a community center in San Bernardino, California, December 4, 2015 (San Bernardino Count Sheriff’s Department / Getty)**

Another aspect of Selim’s work involves reaching out directly to that kid “sitting in the glow of their laptop in their parents’ basement.”

His office has been giving grants and running contests at colleges and universities that form student teams to compete for prizes in internet and social-media messaging aimed at countering ISIL’s online recruiting. “We recognize that government is not a credible messenger for that demographic,” Selim explains. “So we have recruited peer-to-peer messengers.” With the State Department—and Facebook (“to add to the cool factor,” Selim says)—as co-sponsors, he contracted with a private consulting firm that has now persuaded 101 colleges and universities around the world to establish courses, backed by a \$2,000 U.S.-government

stipend per school, offering academic credit to students who create these peer-to-peer anti-jihad social-media campaigns.

Cyberterror

The other hot new threat is cyberterrorism.

Because 87 percent of the country's critical infrastructure is owned by the private sector—power plants, financial institutions, water companies—much of the Department of Homeland Security's lower-profile work involves sharing information and convening forums and sponsoring drills aimed at helping industries help themselves.

Meantime, the government's efforts to protect its own digital infrastructure have provided steady fodder for cynics. To take the latest examples, neither a data-hosting service at the Department of the Interior—whose technology setup was declared by federal officials to be a “Center of Excellence”—nor the Office of Personnel Management detected the hacking in 2014 and 2015 of 25 million records kept by the OPM. A \$1 billion cybersecurity program designed by DHS, called “Einstein,” was, according to the GAO, so ineffective that it missed the hacking of the OPM records. In fact, most government agencies initially defied a presidential directive and refused to even install the much-derided Einstein.

IT'S A BAD SIGN when a program called Einstein turns into a clown show, and it's tempting to make that a metaphor for the government's cybersecurity efforts more generally. However, since taking over DHS's cybersecurity and communications unit three years ago, Phyllis Schneck, a highly regarded cybersecurity engineer who came from the private sector, seems to have put the agency on a better track. She has worked to professionalize the National Cybersecurity and Communications Integration Center, which, although it has produced yet another mind-numbing acronym (NCCIC), has the potential to be effective, according to one Silicon Valley star programmer who has advised the Obama White House on cyberissues. “With

counterterrorism, I have an expectation, and it's met every day, that I will get a full report on threats across the spectrum, because we put in place structures ... to ensure information-sharing across the intelligence community, as well as with state and local law enforcement," says Lisa Monaco, President Obama's White House homeland-security and counterterrorism adviser. "With cyber, we're not there yet, but we're getting there."

Hidden on four floors in a nondescript office building in Virginia (it's not listed in the lobby directory), Schneck's operation includes a heavily guarded floor with space for 150 cyberdetectives, many recruited from the private sector.

Some sit at screens looking for trouble as they monitor the innards of dozens of federal agencies (except the Defense Department, which has its own cybersecurity apparatus). For example, a dramatic upsurge in traffic at the IRS during tax time, in mid-April, would mean nothing, but the same spike on Commerce Department servers could spell trouble.

Others monitor web traffic around the world, looking for similar regional or countrywide anomalies that could indicate attempted sabotage.

**"These savages have so far only figured out how to use the
internet to proselytize ... What happens when they figure
out how to use it to break into a chemical plant, or a
blood bank?," James Comey says.**

Schneck, whose father was a computer scientist at the National Security Agency, describes one approach she is applying as "biological." The Continuous Diagnostics and Mitigation program, for which \$275 million has been budgeted for the coming fiscal year, will reject a virus that makes it onto a government network "in real time, even if we don't know what it is," Schneck says.

Using data-analytics tools from the private sector, she is also augmenting Einstein (which has been allocated \$460 million in this year's budget and \$471 million for next year) with software that will prevent such intrusions in the first place by implementing what she calls "a cyber no-fly list." There are now ways of using data, she explains, to target the address of a machine that has been the source of other hacks, and to keep it from accessing the emails or websites of the agencies she is protecting.

I asked Schneck whether cyberattacks on the government would be impossible or nearly impossible anytime soon. "Of course not," she said. "But we are going to try to stay ahead of them most of the time, and if they do get in, we'll have ways to mitigate, fast. This is not yesterday's government."

Schneck's command center also acts as a real-time clearinghouse for threat information from cybersecurity chiefs in the private sector. The voluntary information-sharing process has been made easier by recent legislation that shields private companies from liability for sharing the information.

For his part, the FBI's Comey worries more about a cyberterror onslaught directed at the private sector than one directed at the government. "These savages," he says, "have so far only figured out how to use the internet to proselytize, not to wreak physical damage. What happens when they figure out how to use it to break into a chemical plant, or a blood bank and change the blood types? We know they are trying. And they don't have to come here to do it."

LAST FALL TED KOPPEL, the former ABC News correspondent and *Nightline* anchor, published *Lights Out*, a short, alarming book that makes the case that the United States is unprepared for a cyberattack on its electric grid. Tens of millions of Americans could be left without power for weeks or even months—and, therefore, also without access to water, ATMs, the towers that transmit their cellphone messages, and other lifelines. Koppel argues that neither the power companies nor the government has sufficient protective measures or backup plans to avert or recover from this kind of disaster.

Because much has improved in the two years since Koppel began his research, the odds of us facing a sustained power outage are lower than Koppel calculates.

To be sure, the power industry has successfully resisted regulations requiring safeguards and backup plans that could render Koppel's book almost moot.

However, with prodding and assistance from DHS's infrastructure-protection office (and obviously wanting to ward off regulation), the industry seems to have taken measures to head off catastrophe. Koppel writes that a smartly directed cyberattack could disable enough giant transformers to cause huge swaths of the country to lose power—and that it would take months to procure and ship replacements to get the grid back online. But according to Gerry Cauley, the president of the North American Electric Reliability Corporation, an industry trade group, there are now reserves of these transformers placed strategically across the country. Moreover, Cauley told me, cyber-repair teams are prepared to spring into action much the way that power-line repair teams from across the country did in response to Hurricane Sandy.

These and other arrangements have been coordinated through DHS's energy-infrastructure-sector team, one of 16 such units covering sectors from information technology to financial services to commercial facilities, such as shopping malls and sports arenas.

The energy-infrastructure team helps organize a biennial attack exercise, during which energy-company executives, along with relevant law-enforcement and other officials, convene for two days to simulate how they would work together in the event of an attack. The most recent exercise, held in November, "stressed us to the point of failure, with multiple cyber- and kinetic attacks across the country," says Thomas Fanning, the chief executive of Southern Company, the giant Atlanta-based utility. In all, more than 4,000 people participated in the exercise. Along with executives and officials in Washington, local law-enforcement and power-company personnel across the country helped defend and recover from simulated cyberattacks, bomb blasts, and gunfire at multiple facilities.

Fanning, an industry leader in cybersecurity, has been a consistent campaign contributor to conservative Republican candidates over the years, which makes this comment notable: “When it comes to these issues, the capability of these government officials in this administration is terrific.”

Part V: The Gaps That Remain

One way to measure how far both DHS and the private sector have come since 9/11 against how far they still need to go is to imagine the inevitable report citing our next failure of imagination, much the way that the bipartisan panel organized by Scooter Libby last year reminded us of the threat of a catastrophic bio attack. It’s a parlor game that’s easy to play; we can never be completely safe from people who are willing to commit suicide to hurt us. Yet it’s worth playing not only because some vulnerabilities are far more serious and likely to be exploited than others, but because the two most-talked-about threats of the moment—lone wolves and cyberterrorism—so dominate headlines that they may have unduly diverted our focus from bigger dangers. As Tom Ridge told me, “Democracies tend to be reactive, not prescriptive, and that’s a homeland-security problem that will be with us forever.”

Exploiting some of our vulnerabilities requires more expertise and planning than a one-off shooting spree in a mall. However, the small groups necessary to take advantage of them could easily be trained in countries where ISIL, or new groups we haven’t heard of yet, hold territory. And, of course, they could be homegrown.

Many such threats remain, including the bioterror attack that the Libby panel warned of last year. The potential for sabotaging a freight train carrying oil or toxic chemicals, which could kill thousands, would also be on my list.

But my reporting leads me to conclude that the most ominous terrorist threat—based on the relative ease of pulling off such an attack, the possible damage it could do, and, most of all, the danger of overreaction to it—is the dirty bomb.

The Bomb That Lasts for Decades

In March 2002, Joe Biden, who was then the chairman of the Senate Foreign Relations Committee, held a hearing in which the president of the Federation of American Scientists used a study recently completed by his organization to describe a doomsday scenario unfolding a few blocks from Capitol Hill.


Biden had convened the committee to hear testimony about the threat of dirty bombs—a conventional explosive mixed with commonly available radiological material, such as that used in hospitals and industrial facilities. Henry Kelly, then the president of the federation, which was formed by scientists in 1945 to study ways to prevent nuclear catastrophes, described for the committee what would happen if a small conventional bomb mixed with a small amount of cesium-137—which can be found in everything from nuclear reactors to radiation therapy for cancer patients—were set off at the National Gallery of Art. The explosion might kill only a few people, but it would create an area with contamination levels as dangerous as a “Superfund” site—a venue designated as having high levels of toxic waste that demand immediate government intervention and often evacuation. The contaminated area would cover 40 city blocks that include the Supreme Court, the Library of Congress, and the Capitol. Those buildings could have to “be abandoned for decades,” Kelly warned.

According to Kelly, an extra one in 10,000 people would die of cancer if people were not evacuated and if the area were not completely scrubbed. The decontamination process could take years and cost billions, because radioactive material adheres stubbornly to cement, which means that many roads, sidewalks, and buildings would have to be replaced.

However, that prospective death toll is worse than it sounds. Indeed, as the hearing proceeded, it became clear that dirty bombs present less a safety challenge than a perception challenge. In a city of 500,000, the contamination level Kelly cited would mean an extra 50 cancer deaths over a period of years—an incremental

casualty rate that could probably be offset by an antismoking campaign in one or two D.C. office buildings.

Even concentrations of radiation higher than what Kelly posited would still not endanger masses of people. But because of popular perception, an explosion would unleash panic—which is why many experts are surprised that a dirty-bomb attack has not happened.

 **There were 325 reported instances of nuclear or radiological material being lost or stolen in 2013 and 2014. This material could easily be used to build a dirty bomb. Sometimes only a cheap padlock stands between would-be terrorists and radioactive material. (Government Accountability Office)**

The ingredients are readily available. According to a recent white paper from the Nuclear Threat Initiative (NTI)—the nonprofit dedicated to fighting proliferation founded by Ted Turner and Sam Nunn, the former Democratic senator from Georgia—“the ingredients for a radioactive dirty bomb are in tens of thousands of radiological sources located in more than 100 countries around the world.” The report cited a database that had documented 325 instances of nuclear or radiological material having been publicly reported lost or stolen in 2013 and 2014 alone. And those are just the publicly reported losses and thefts.

The release of the NTI's white paper was timed to coincide with the Nuclear Security Summit hosted by President Obama in March. This was the last of a series of meetings of world leaders that Obama had initiated in 2010 to address nuclear proliferation. Lately, the threat of dirty bombs—whose radiological material isn't potent enough to make actual nuclear weapons—has become a significant part of the nuclear-security agenda. Twenty-three of the summit's 52 countries, including the United States, have made commitments, according to the NTI, "to secure their most dangerous radiological sources."

That's significant progress, and it has been accompanied by clandestine efforts around the world by U.S. and allied counterterror agents who, I learned in reporting this story, have blocked multiple attempts by would-be terrorists to obtain radiological material and, in some cases, nuclear material. But if only 23 countries have committed to securing their radioactive material, that leaves most of the world uncommitted to securing widely dispersed ingredients for dirty bombs.

Last October, DHS officials testified before a House transportation subcommittee on whether someone from one of those countries could ship such material through an American port. They tried to put the best gloss on a scary reality. Todd Owen, a Customs official, said that all 11 million containers arriving at U.S. seaports are "analyzed" and "screened." What he meant was that all containers are subject to a data-based threat matrix. Scanning every container—which is what that Customs supervisor at the New Jersey port wanted to do on the afternoon of September 11—at least with X-rays, if not by hand-searching them, was mandated by Congress in 2007. But it has never been done for every container—and arguably can't be done, given the delays in international commerce such a process would precipitate. Only about 3 percent of containers (those that register high on the threat matrix) are now X-rayed.

One hundred percent do pass through some kind of radiation monitor, Owen said—but those monitors cannot detect radiological material wrapped in lead or other protective covering. This is why the thousands of small radiation monitors that police in cities like New York now carry may be an important tool for detecting

unshielded illicit material, but are unlikely to detect a dirty bomb, because the low levels of radiation necessary for such a device are not difficult to shield. The shielding material could likely be detected in an X-ray—but, as noted, only about 3 percent of containers are X-rayed.

Moreover, hundreds of thousands of a different kind of potential container—cars coming into American ports from factories abroad—are never X-rayed at all or subject to any kind of actual threat-matrix analysis.

I asked John P. Wagner, a deputy assistant Customs commissioner, why a terrorist couldn't simply put shielded dirty-bomb material in the trunk of a BMW. Wagner explained that car exporters are in his agency's "trusted shipper" program, meaning that "we inspect those factories regularly to make sure they have adequate security plans in place." When I followed up and asked for details about the last time Customs had inspected an auto factory, Wagner's office said there was no record of any such inspection.

S O IT DOESN'T REQUIRE a wild leap to imagine someone with terrorist sympathies planting shielded radioactive material in a car or a cargo container that then makes its way through one of our ports. But it's even easier to imagine a dirty bomb being constructed from material that doesn't have to be snuck through the ports—because, despite significant work done by the Obama administration, large quantities of radioactive material already sit unguarded in the U.S.

According to the National Nuclear Security Administration (NNSA), approximately 1,400 industrial facilities in the United States house high-risk radiological sources. The material is used for everything from testing the ground for oil drilling to irradiating food in order to kill germs. In addition, some 1,500 hospitals and other medical facilities use high-risk radiological material.

Responsibility for guarding this material is split between the NNSA, a unit of the Energy Department, and the Nuclear Regulatory Commission (NRC).^{**} According to multiple GAO reports, efforts to secure radioactive material have been

hamstrung by turf battles between the two agencies. The NRC regulates all entities that use radiological material and imposes security requirements on them. But those requirements have been consistently criticized by independent security experts—and by the government’s own experts at the NNSA—as dangerously lax.

“We choose not to be prescriptive in our regulations,”
says the head of the Office of Nuclear Material Safety and
Safeguards. “We take a more general approach, offering
guidelines.”

The NNSA is responsible for maintaining the safety of the American nuclear arsenal and also for providing expertise related to counterproliferation. In that context, it conducts security surveys and encourages facilities to enforce standards that are much tighter than those required by the NRC. But the NNSA itself can impose no security requirements.

If a dirty bomb goes off in Washington or on Wall Street, the question of why the standards that one federal agency (the NNSA) believes are necessary are higher than those of the federal agency (the NRC) that can actually regulate toxic material will no doubt be the subject of another blue-ribbon commission.

What this new commission will find is that once the adrenaline flowing from the September 11 attacks receded, the industries licensed by the NRC began to push back against those sounding the terror alarm.


“The NRC is basically a captive of the industry,” says Andrew Bieniawski, a veteran proliferation expert who is the vice president for material security and minimization at the Nuclear Threat Initiative. “They get 90 percent of their funding from licensing fees from the industry, and they’re always saying they’re worried that tougher requirements would put licensees out of business.”

“Just a Matter of Time”

The NNSA has persuaded 796 of the 1,503 hospitals that use radiological material to implement security upgrades that extend well beyond the NRC’s vague requirements. That is a major improvement; in 2012, the GAO noted that only 321 hospitals had made these upgrades. Other hospitals and medical facilities have been persuaded to make the transition from high-risk material to newer, safer substitutes. But that still leaves hundreds of medical facilities with threadbare security, many in highly populated urban areas.

It is astonishing that so many hospitals have refused to spend what Bieniawski says is the \$300,000 to \$400,000 necessary per site to increase security, and the \$250,000 necessary to replace a cesium-chloride blood irradiator with an equivalent FDA-approved nonradiological device, especially because the hospitals that use this material for advanced treatments are typically large enterprises with tens of millions of dollars in annual operating profit.

“It’s just a matter of time until someone puts two and two together and sees that you don’t have to go to Syria or Iran for this material, that you can get it in New York,” Bieniawski says.

 **Shipping containers at Maher Terminals in Elizabeth, New Jersey. Screening such containers for dirty-bomb material remains a challenge for DHS and local law enforcement. (Mark Lennihan / AP)**

Nonmedical industrial users remain an even bigger threat. In 2014, the GAO issued a report that will be another proverbial smoking gun if something catastrophic happens. Independent auditors roundly criticized the NRC's regulations as weak and inconsistently enforced. Some trucks carrying radiological devices used by oil-drilling companies, for example, were found to have cheap padlocks to secure the equipment. Background checks of drivers and warehouse employees were not standardized. GPS devices for the trucks, which could track them down if they were stolen, were not required. Storerooms containing material that could be used to turn Disney World into a ghost town had no entry alarms and were protected by simple padlocks—if they were locked at all. Even when storerooms and trucks did have alarms, many were found to be inoperable or shut off. After a truck went missing in Washington State, the governor's request to get the NRC to require GPS devices was rejected.

“We choose not to be prescriptive in our regulations,” Scott Moore, the acting director of the NRC's Office of Nuclear Material Safety and Safeguards, told me when I asked about the GPS requirement. “We take a more general approach, offering guidelines,” which he believes “are adequate to assure public health and safety.” As for the apparent disconnect between the security measures the NNSA believes are necessary and the NRC's requirements, Moore said, the “NRC's approach provides adequate security; NNSA's suggestions are for additional security.”

Part VI: The End of “Never Again”

The TSA spends about 98 percent of its budget on one transportation sector, aviation. Why does it make sense to screen airplane passengers and not the millions

more people getting on trains and subways every day? And why place all those resources at our big freight ports when a pleasure boat carrying a dirty bomb can arrive in Florida from the Bahamas with no inspection? What about the ferries that each haul thousands of people through the waters off New York City and Seattle? A well-placed explosive could kill many more people on a train or boat than on a jetliner.

In May, the inspector general of DHS sharply criticized the TSA for failing to implement legislation passed in 2007 requiring a variety of security measures for Amtrak, including checking to see if railroad employees were on terrorist watch lists. In response, the TSA promised that it had “assigned the highest of priorities” to implementing the nine-year-old law. However, the reality is that although we have stepped up police monitoring of trains (and ferries), we can’t treat trains like planes.

Why not? The math doesn’t allow it. The New York City subway system has about as many entrances as there are checkpoints at all the airports in the country. To secure the subways in New York, we would have to create a whole other TSA. Beyond the \$7-billion-a-year tab that would come with a New York TSA, the new security process would probably double travel times. (Imagine: shoes off before boarding the subway.) It’s such a ridiculous notion that even typing this paragraph is embarrassing.

The security measures that do make sense are those that local and federal officials implemented after 9/11 to make the subway tunnels more secure, helping to ensure that a potentially catastrophic September 11-level massacre following a huge explosion and subsequent flood is more likely to be limited to a routine semi-mass casualty.

Routine?

I use the word deliberately.

The morning after 9/11, President Bush famously directed then-Attorney General John Ashcroft to make sure “this can’t happen again.” It was an understandable

sentiment. But it was a fantasy then—and it is even more of a fantasy now, despite everything we’ve done.

The reality we face 15 years after the September 11 attacks is that for all the people and money we have thrown at the cause of “never again”—much of it heroically and wisely, and much that in hindsight looks desperate, stupid, or corrupt—the threat of terror hasn’t been eliminated. In fact, despite our best efforts, terror is destined to become, yes, routine—a three- or four-times-a-year headline event, perhaps almost as routine in this country as people with mental-health problems buying a semiautomatic and going hunting at a school or movie theater. But if, as seems to be the case, Americans have come to accept mass killings carried out by those who are mentally unstable as horrifying but not apocalyptic, why do they perceive an attack linked—even if just rhetorically by the perpetrator—to Islamist terrorism differently?

President Obama described the difference to me this way: “If the perpetrator is a young white male, for instance—as in Tucson, Aurora, and Newtown—it’s widely seen as yet another tragic example of an angry or disturbed person who decided to lash out against his classmates, co-workers, or community. And even as the nation is shaken and mourns, these kinds of shootings don’t typically generate widespread fear. I’d point out that when the shooter or victims are African American, it is often dismissed with a shrug of indifference—as if such violence is somehow endemic to certain communities. In contrast, when the perpetrators are Muslim and seem influenced by terrorist ideologies—as at Fort Hood, the Boston Marathon bombing, San Bernardino, and Orlando—the outrage and fear is much more palpable. And yet, the fact is that Americans are far more likely to be injured or killed by gun violence than a terrorist attack.”

The FBI’s Comey agrees. “That the shooter in San Bernardino said he was doing it in the name of ISIL changed everything,” he told me. “It generates anxiety that another shooting incident, where the shooter isn’t a terrorist, doesn’t. That may be irrational, but it’s real.”

In that instance, the sheer ordinariness of the venue—a meeting room at a family-services center—exacerbated the anxiety. “For me, San Bernardino was the game changer,” Ray Kelly, the former New York City police commissioner, told me. “It put the whole country in the target zone.”

 **Attorney General John Ashcroft listens as President George W. Bush speaks prior to signing an anti-terror bill, July 15, 2004. (Brooks Kraft / Corbis / Getty)**

“Engineering Security,” the manual that Kelly’s department published in 2009, urged building owners to consider the status of their venue in assessing how much protection it needed. Iconic structures or those housing high-profile businesses should be the most fortified, as should those where an attack could cause inordinate damage.

That ranking system still makes sense, “but the kind of place attacked in San Bernardino means that everything is a target,” Kelly explained. “The FBI and the NYPD can do a great job finding and rolling up some people who are even thinking about doing something bad, but they can’t find everyone, and they can’t be

everywhere. Imagine if just a few of these people got together and shot up a few malls the same day around the country. Then no one would feel safe.”

Yes, we can take steps to harden those softer targets a bit. We can improve surveillance technology and add guards. We can keep doing our best to identify those among us who are susceptible to online jihadist recruitment pitches, by persuading neighbors and family members who “see something” to “say something.” We can keep improving how we connect the intelligence dots around the world.

But there is a limit. We can’t turn every Macy’s or high-school basketball game into a TSA operation.

And even if we did, those terrorists who don’t care about dying—for whom there is no such thing as deterrence—will still shoot people on the street.

Or bomb them. Or use a truck to mow them down.

We have to accept that that is going to happen.

A favorite September 12 mantra in the anti-terror community is: “The terrorists have to be right only once—but we have to be right 100 percent of the time.”

We can’t be right 100 percent of the time. The FBI and the Joint Terrorism Task Forces have stopped between three and five dozen plots since 9/11, depending on one’s definition of a plot. Comey’s “well-oiled anti-terror machine” has indeed improved our defenses. And the TSA, Customs, the air marshals, and other DHS units have undoubtedly deterred attacks. But we can’t catch everything.

Layers

That’s why those in the anti-terrorism business focus on another post-9/11 buzz phrase: *layers of security*.

When it comes to flying, that means first checking prospective passengers' watch-list status. Then, when passengers arrive at the airport, undercover security agents look for suspicious people in the departure lobby. That's a layer now being fortified following the Brussels and Istanbul airport bombings, although it is difficult to see why airport lobbies should get more security attention than other similarly crowded venues.

The third layer is at the security checkpoint, where passengers are screened for valid identity credentials and to make sure they are not carrying anything dangerous. Fourth, an air marshal might be on board the plane to interrupt a possible attack. The fortified cockpit door offers a final security layer. The fact that we have all these layers is our tacit admission that no single layer of defense is perfect—but the odds of getting through all of them, while not zero, are pretty steep.

Think of the process as a funnel, in which we start with a large population and whittle it down, layer by layer, to those allowed to board a plane. "Sometimes I think that the lid has come off the world," Comey told me. "People are unsettled, unmoored. I worry that as we squeeze ISIL in Syria—and we are—their troops will go to Libya or Europe," he continued. "There will be a terrorist diaspora. Trained fighters will go there and then be more easily able to come here, or if they can't get here directly they'll get to Canada and try to drive over the northern border."

That so many could pour into the top of the funnel—including those recruited online, at home in America, without having to cross any border—is as important in calculating our odds of avoiding an attack as assessing the remaining gaps in even our most porous layers.

The New Reality

Those who have enlisted since 9/11 to maintain those security layers—the infrastructure-security coaches at DHS advising and cajoling stadiums, utilities, water plants, and other private-sector venues; the TSA airport screeners; the

cyberdetectives; the FBI dot-connectors—have no control over how many would-be killers pour into the top of that funnel. And they get little attention from the rest of us until something goes wrong. We go about our lives oblivious to the threats that are their obsession—until the next catastrophe produces headlines. Meantime, we often dismiss their work that is visible to us, such as at the airports, as excessive. Yet we remain so ready to be retroactively indignant if something goes wrong that political leaders, encouraged by a Beltway culture that tries to keep the spigot always turned on, are afraid to make any choices other than to declare everything a priority.

Sooner or later we have to realize that “never again” is a fantasy, and that it is not an excuse to make everything a priority. A democracy must make rational decisions, even when that’s not easy, and especially when security is involved.

Can the tens of billions for FirstNet or for “homeland security” grants for toys like that monster fire truck in rural Virginia be justified as smarter investments than replacing the lead pipes in a significant portion of the nation’s water systems? Wouldn’t the \$800 million a year for air marshals be better spent on more TSA staffing to cut wait times? Can’t we have tougher procurement contracts, so that Boeing and Lockheed Martin would have to give the money back when their products don’t work, so the country could direct those billions to hiring more FBI agents or perhaps to expanding early-childhood education?

Conversely, does it make sense that Congress has decided that giving everyone, including deranged people and terrorists, free rein to buy assault weapons at gun shows is the one situation where “never again” is not the highest priority?

G


ETTING PAST “NEVER AGAIN” doesn’t just mean making tough choices about priorities; it also means preparing for the inevitable.

In theory, a realistic approach should be uncontroversial. For example, conceding the usefulness of drills because some attacks will inevitably succeed is not an admission that we don’t care about prevention, any

more than having ambulances on call is a sign that we don't care about preventing traffic accidents or violent crime.

But when it comes to terrorism, the balance between prevention and accepting the reality that prevention will not always work is trickier.

President Obama is the first post-9/11 president, and he and his administration have made significant, if often muted, progress in adding two dimensions to the homeland-security mission beyond the first goal of prevention: mitigation (lessening damage from a successful attack) and recovery.

 **Oklahoma Senator Tom Coburn, who has criticized DHS for wasteful spending, introduces a report on the defense budget, November 15, 2012. (Chris Maddaloni / CQ Roll Call / Getty)**

In his 2015 report on DHS, Senator Coburn demonstrated how officials who make mitigation and recovery a priority can be political targets. He acknowledged that the terrorism drill conducted in Boston before the marathon bombing might have played a “constructive” role, but he criticized a DHS report about the drill because

it suggested that the Obama administration was more focused on “preparing state and local first responders for the emergency and swift response” than on “what additional roles DHS could play in preventing future terrorist attacks.” That “raises questions,” Coburn concluded, about whether “terrorism prevention truly is the Department’s first mission and whether that mission has been transformed into preparing to recover from terrorist attacks.”

I asked President Obama about Coburn’s critique. “Part of keeping the American people safe is making sure we’re ready for all contingencies,” he told me. “So it’s not ‘either/or’—preventing attacks or being able to respond to and recover from attacks. We have to do both. In fact, to focus solely on prevention while ignoring response and recovery—or vice versa—would be irresponsible.”

“After all,” President Obama continued, “from Boston to San Bernardino to Orlando, we’ve seen how important it is for communities and first responders to be ready if and when tragedy strikes. That’s a critical part of preventing attacks from causing even greater loss of life. It’s a key part of our resilience. It’s one of the ways we can show terrorists that they will not succeed—that Americans get back up and we carry on, no matter what.”

M

ITIGATION AND RECOVERY need to be about more than repairing physical damage. After all, terrorism’s first goal is inflicting psychic damage—scaring us into changing our way of life and even turning against one another.

President Bush’s strategy was simply to tell us not to worry—that we should fearlessly keep on shopping. As a short-term measure, it was a sensible effort to calm a shocked nation. But the longer term requires a more nuanced, and politically perilous, message, because there is no such thing as “never again.” Attacks will happen, and, as San Bernardino and Orlando portend, they will happen in random venues—where part of what’s so frightening is the randomness, suggesting that anyone, anywhere, anytime could be vulnerable.

In the April issue of this magazine, Jeffrey Goldberg reported that President Obama “frequently reminds his staff that terrorism takes far fewer lives in America than handguns, car accidents, and falls in bathtubs do.” Goldberg also wrote that the president had frequently expressed to him “his admiration for Israelis’ ‘resilience’ in the face of constant terrorism, and it is clear that he would like to see resilience replace panic in American society.”

When *The Atlantic* published this account, Obama was immediately attacked by Republicans in Congress and on the presidential campaign trail for not taking terrorism seriously and for admitting defeat.

“President Obama’s job is to keep us safe,” Tom Cotton, a Republican senator from Arkansas, said on *Morning Joe*. “It’s not to minimize the fear Americans justly fear about terrorism ... President Obama goes around telling people that more Americans die in bathtub falls than are killed by terrorists. It’s that mentality that we have to change and get on offense against the Islamic State if we don’t want to see a Brussels-style attack here.”

One of Obama’s senior security advisers countered in a conversation with me: “If we overreact to these relatively small attacks, it creates more incentive for someone else to try one, but that’s what the media does and what most politicians do.

“What if those militiamen who took over that park in Oregon had been Muslims? We’d have had wall-to-wall coverage,” the adviser added. “The president sees trying to get Americans to take a more nuanced view of terror as part of his job.”

Dirty Bombs

Obama’s ambition to give Americans a realistic understanding of terror threats is certainly more advanced than his predecessor’s “never again” posture. But when it comes to the weapon in the terrorist arsenal that is most about perception versus reality—the dirty bomb—he has recognized the problem yet fallen short of the challenge.

Beyond forcing his Nuclear Regulatory Commission to promulgate security regulations at least as strict as the measures his National Nuclear Security Administration is stuck trying to persuade custodians of radiological material to adopt, the president ought to launch an education campaign about dirty bombs from his own bully pulpit. Removing the public's untoward fear of the bomb can defuse its power to terrorize.

The Bush administration's sole contribution to public understanding of dirty bombs went in the opposite direction. In 2002, when John Ashcroft announced the detention, with no hearing or charges brought, of José Padilla, an American citizen, for allegedly being part of "an unfolding terrorist plot" to detonate a dirty bomb (an allegation later dropped for lack of evidence), he sought to justify depriving Padilla of due-process rights by warning that a dirty bomb could cause "mass death and injury." Tom Ridge, as well as two senior members of Bush's White House staff, told me at the time that they were appalled by Ashcroft's hyping of the danger, though they did nothing publicly to correct his message.

President Obama and his administration obviously understand the perception problem. In 2013, the Environmental Protection Agency, in a move coordinated by the National Security Council, softened its Protective Action Guides related to radiation incidents. These are the radiation metrics, originally published by the EPA in 1992, that first responders would use to determine what area, if any, had to be evacuated in the event of a radiological-contamination event. With the change in these guidelines, the bomb hypothesized in the 2002 Senate testimony of the Federation of American Scientists president—which would have forced the abandonment of a 40-block area around Capitol Hill—might now dictate the clearing of a smaller area or no area at all, depending on the type of bomb.

The guideline revisions, which were published in the Federal Register, cited advances in understanding the science of radiation and also a new focus on a "broader range of radiological emergencies, including terrorist acts."

What that means, according to a senior White House security official, is that the Obama administration decided that the original guidelines for handling the

aftermath of a dirty bomb's detonation were unreasonably extreme—that evacuating downtown Washington to avert the possibility of 50 cancer deaths would be an absurd overreaction.

All of which makes sense—except that the Obama administration squandered an opportunity by flinching when it came to announcing the change. There was no press release. No public explanation at all. Just changes described mostly with physics jargon and numbers dropped into the Federal Register. As a result, what could have been an ambitious, gutsy exercise in public education—a “teachable moment”—now risks being discredited as an anticipatory cover-up if a dirty-bomb attack occurs. Breathless press reports will “reveal” that the guidelines were changed sub rosa, and that—based on the guidelines in place before President Obama’s staff quietly tinkered with them—much of Washington is being asked to live and work atop land as dangerous as a Superfund site. In the aftermath of a dirty-bomb explosion, explaining the guideline changes in a way that calms anyone would likely be impossible.

**The president has failed to finish the job of securing
radiological material in hospitals and other facilities—
and taken only tentative steps toward leveling with the
public.**

Following Donald Trump’s criticism of President Obama and Hillary Clinton in the wake of the Orlando massacre for not being “tough,” political commentators called the attack a “June surprise” that could affect the presidential election. Imagine the eruption from the Trump campaign that could come from an administration attempt to explain the loosened guidelines the day after an ISIL-inspired group used a dirty bomb as the ultimate October surprise aimed at disrupting the coming election.

“People inside and outside the government who worked on these guidelines went back and forth over whether to announce it or bury it, and they decided to bury it,” says Charles Ferguson, who, as the president of the Federation of American Scientists, now occupies the post previously held by Henry Kelly, who laid out the Washington evacuation scenario during the 2002 Biden Senate hearing. “On the merits, they did everything right—but then they went into duck-and-cover mode.”

When I asked President Obama why his administration didn’t announce the change in guidelines and use it as an opportunity to begin a public discussion about dirty bombs, he referred me to Laura Holgate, a senior National Security Council official. Holgate provided a statement saying that publishing the revisions in the Federal Register had attracted “public comment” from interested parties and was a “normal process” that was “not, in any way, secret.”

H

OW WASHINGTON HAS COPED with the threat of dirty bombs is a microcosm of how the country has dealt with terror overall in the past 15 years.

First, by bringing proliferation to the international stage through the summits he has hosted, Obama improved on his predecessor’s prevention efforts—much as he has done by hunting down terrorist leaders abroad while hardening targets and tightening homeland-security management at home.

 **President Obama walks past a televised image of President Bush at the opening of the 9/11 Memorial, 10 years after the attacks. (James Leynse / Corbis / Getty)**

However, the president has failed to finish the job of securing radiological material in hospitals and industrial facilities, or to crack down on the threats from bioweapons and toxic chemicals. Second, with his revised EPA guidelines on dirty-bomb damage, Obama has taken a tentative but insufficient step toward leveling with the public in a way that deprives terrorists of their ability to spread hysteria. That mirrors what he has tried to do more generally: tentatively steer Americans toward the realistic view that while terrorism is inevitable, it is not an existential or apocalyptic threat—unless we treat it like the apocalypse.

This is a politically perilous path—which may explain why the administration proceeded so quietly when announcing the revised radiological-contamination guidelines.

In fact, this may be a path only a lame duck could risk. The politically easier path is to promise “never again.” As Trump’s hard-line rhetoric about the president being weak on terrorism demonstrates, Obama and anyone who follows him and tries to continue on that path will be an easy target for opponents who will claim that transforming homeland security from the fantasy of never-again prevention to a combination of prevention and mitigation and recovery is throwing in the towel.

That this is still a debate in an election season 15 years after the 9/11 attacks is evidence that although we’ve made progress, we’re still a long way from adjusting—politically and psychically—to this new normal, where, unlike during the Cold War, there is no relying on deterrence for protection.

* This article originally stated that the Attack 2 truck was paid for with a \$185,000 federal homeland-security grant. In fact, the grant was \$160,000. The total cost of the truck is \$375,000, and the fire department is covering the remainder. We regret the error. [^]

** This article originally stated that the Nuclear Regulatory Commission is a unit of the Energy Department. We regret the error. [^] *A*

ABOUT THE AUTHOR

STEVEN BRILL is the founder of *The American Lawyer* and CourtTV. He is the author of *America's Bitter Pill: Money, Politics, Backroom Deals, and the Fight to Fix Our Broken Healthcare System*.
