The New York Times

Turning the Page on an Open Checkbook for the Security Colossus

By: SCOTT SHANE - October 24, 2012

WASHINGTON — Last week, a Bangladeshi student was charged in an F.B.I. sting operation with plotting to blow up the Federal Reserve Bank in New York. A Somali-American man was convicted of sending young recruits from Minneapolis to a terrorist group in Somalia. In Libya, extremists responsible for the killing of four Americans last month in Benghazi remained at large.

The drumbeat of terrorism news never quite stops. And as a result, for 11 years since the Sept. 11 attacks, the security colossus constructed to protect the nation from Al Qaeda and its ilk has continued to grow, propelled by public anxiety, stunning advances in surveillance technology and lavish federal spending.

Now that may be changing. The looming federal budgetcrunch, a sense that major attacks on the United States are unlikely and new bipartisan criticism of the sprawling counterterrorism bureaucracy may mean that the open checkbook era is nearing an end.

While the presidential candidates have clashed over security for American diplomats in Libya, their campaigns have barely mentioned homeland security. That is for a reason: less than one-half of 1 percent of Americans, in a Gallup poll in September, said that terrorism was the country's most important problem.

But the next administration may face a decision: Has the time come to scale back security spending, eliminating the least productive programs? Or, with tumult in the Arab world and America still a prime target, would that be dangerous?

Many security experts believe that a retrenchment is inevitable and justified.

"After 9/11, we had to respond with everything we had, not knowing what would work best," said Rick Nelson, a former Navy helicopter pilot who served in several counterterrorism positions and is now at the Center for Strategic and International Studies. "That's a model we can no longer afford, financially or politically."

Michael V. Hayden, who led both the National Security Agency and the Central Intelligence Agency in the years after the Sept. 11 attacks, agrees that the time will come for security spending to be scaled back and believes that citizens need to decide when that should happen. Personally, he would wait a while longer.

"I would stand fast for now," said Mr. Hayden, who is an adviser to Mitt Romney.

In the view of most specialists, the danger to United States territory from Al Qaeda and its allies is far less than it was in 2001. Al Qaeda's leaders have been relentlessly hunted, its ideology was rejected by most of the young Muslims who led the Arab revolts, and its recruits in the United States have been few. Of more than 160,000 homicides in the country since Sept. 11, 2001, just 14 were carried out by Qaeda sympathizers in the name of jihad.

Some of the credit is no doubt due to homeland security programs that cost taxpayers about $690 billion over the decade after the Sept. 11 attacks, according to John Mueller, a political scientist at Ohio State University. That money has paid for an alphabet soup of new agencies: the Department of Homeland Security, the Office of the Director of National Intelligence, the National Counterterrorism Center, the Terrorist Screening Center and many others, each with a supporting cast of contractors. Old agencies like the C.I.A. and the F.B.I. have bulked up, and a record 4.8 million people hold security clearances.

Yet any move to trim the counterterrorism bureaucracy will face daunting opposition. Some Americans will worry that cutbacks could put them at risk. Members of Congress will fear being labeled soft on terrorism. Lobbyists will fight to protect the lucrative homeland security sector.

For years, counterterrorism programs have been met mostly with cheerleading on Capitol Hill, despite billions spent on programs that turned out to be troubled or ineffective: "puffer" machines for airport screening that were warehoused, a high-tech surveillance program on the border with Mexico that was shut down, costly machines to sniff city air for biological weapons that produced too many false positives.

No previous Congressional criticism of counterterrorism programs, however, has been quite so scathing as a bipartisan Senate subcommittee report this month on more than 70 “fusion centers” nationwide, created to help federal, state and local authorities share threat information. The two-year investigation found that the centers had failed to help disrupt a single terrorist plot, even as they spent hundreds of millions of taxpayer dollars and infringed on civil liberties.

But the reaction to the report illustrated why it will be difficult to cut even marginal programs. Senior senators, the Department of Homeland Security and a half-dozen law enforcement groups rushed to criticize the report and defend the centers, which, not coincidentally, provide jobs and spending in every state.

Philip B. Heymann, a Harvard law professor and a former deputy attorney general, said that after every war there had been an adjustment that shrank the security establishment and eased wartime controls to restore a traditional balance of power between the government and the citizenry.

“If you want the America we built over 200 years, we always have to be looking for ways to ratchet back these controls when it’s safe,” said Mr. Heymann, who is writing a book on the subject. “If we tried, we could find a number of places where we could move back toward the normal of 2000 without reducing security.”

Like other intelligence officials after 2001, Mr. Hayden was whipsawed by public wrath: first, for failing to prevent the Sept. 11 attacks, and then, a few years later, for having permitted the National Security Agency to eavesdrop on terrorism suspects in the United States without court approval.

Perhaps, as a result, he often says that the American people need to instruct the government on where to draw the line. He told an audience at the University of Michigan last month, for instance, that while a plot on the scale of the Sept. 11 attacks was highly unlikely, smaller terrorist strikes, like the shootings by an Army psychiatrist at Fort Hood in Texas in 2009, could not always be stopped.

“I can actually work to make this less likely than it is today,” Mr. Hayden said. “But the question I have for you is: What of your privacy, what of your convenience, what of your commerce do you want to give up?”

A big problem for Mr. Hayden’s formula is government secrecy, which makes it tough for any citizen to assess counterterrorism programs, their value and their intrusion on people's privacy. Ubiquitous new technology has made it far easier for agencies to keep watch on Americans, using cellphones that track location, Internet monitoring, video surveillance cameras, facial recognition software and license plate readers. And the government increasingly taps into the huge amounts of data that companies gather.

"I think the greatest threat to privacy these days is the enormous amount of data in the hands of private companies that could be misused — either by the government or by companies," said John Villasenor, an electrical engineer at the University of California, Los Angeles, who studies the social impact of technology. "Today almost everything we do is recorded by default."

Consider the counterterrorism databases that the F.B.I. has built, largely in secret, with names like Investigative Data Warehouse and Foreign Terrorist Tracking Task Force Data Mart. One public glimpse — a heavily redacted 2006 list of materials in the Data Mart obtained by Wired magazine under the Freedom of Information Act — suggests the sweep of information being gathered: sprawling data collections from dozens of government agencies, on subjects like suspicious bank transactions and lost passports; voluminous records from commercial data collectors like Acxiom, ChoicePoint and Accurint (which alone accounted for 175 million entries); even hotel guest records.

An F.B.I. spokesman, Christopher M. Allen, declined to provide a current list of data in the system. But he said F.B.I. rules gave "greater overall protections for privacy than the law requires" and were strictly enforced by bureau lawyers.

Such official assurances do not comfort civil libertarians. Marc Rotenberg, the executive director of the Electronic Privacy Information Center, a Washington watchdog group, said that the easing of government incursions on privacy and rights that traditionally followed a war may not come this time, because the technology-driven "architecture of surveillance and security" remained in place.

"We're still left with this largely unaccountable infrastructure," Mr. Rotenberg said. "As long as we don't begin to dismantle that, I'm not sure we will ever move past 9/11."