Recalibrating Homeland Security

Mobilizing American Society to Prepare for Disaster

Stephen Flynn

The United States has made a mess of homeland security. This is hardly surprising. The policymakers responsible for developing homeland security policy in the wake of September 11, 2001, did so under extraordinary conditions and with few guideposts. The Bush administration's emphasis on combating terrorism overseas meant that it devoted limited strategic attention to the top-down law enforcement and border-focused efforts of the federal departments and agencies assigned new homeland security responsibilities. President Barack Obama has largely continued his predecessor's policies, and congressional oversight has been haphazard. As a result, nearly a decade after al Qaeda struck the World Trade Center and the Pentagon, Washington still lacks a coherent strategy for harnessing the nation's best assets for managing risks to the homeland—civil society and the private sector.

For much of its history, the United States drew on the strength of its citizens in times of crisis, with volunteers joining fire brigades and civilians enlisting or being drafted to fight the nation's wars. But during the Cold War, keeping the threat of a nuclear holocaust at bay required career military and intelligence professionals operating

---

Stephen Flynn is President of the Center for National Policy.

within a large, complex, and highly secretive national security establishment. The sheer size and lethality of U.S. and Soviet nuclear arsenals rendered civil defense measures largely futile. By the time the Berlin Wall came down and the Soviet Union collapsed, two generations of Americans had grown accustomed to sitting on the sidelines and the national security community had become used to operating in a world of its own.

To an extraordinary extent, this same self-contained Cold War–era national security apparatus is what Washington is using today to confront the far different challenge presented by terrorism. U.S. federal law enforcement agencies, the border agencies, and the Transportation Security Administration (TSA) are subsumed in a world of security clearances and classified documents. Prohibited from sharing information on threats and vulnerabilities with the general public, these departments' officials have become increasingly isolated from the people that they serve.

This is the wrong approach to protecting the homeland. Even with the help of their state and local counterparts, these federal agencies cannot detect and intercept every act of terrorism. Police, firefighters, and other emergency responders will not always be immediately at hand to protect and rescue those in harm's way. Professionals are usually not the first responders to terrorist attacks and other disasters. A sidewalk T-shirt vendor, not a police patrol officer, sounded the alarm about Faisal Shahzad's SUV in his May 2010 car-bombing attempt on New York's Times Square. Courageous passengers and flight-crew members, not a federal air marshal, helped disrupt the suicide-bombing attempt by Umar Farouk Abdulmutallab aboard Northwest Airlines Flight 253 on Christmas Day 2009. It often falls to ordinary citizens—family, friends, neighbors, and bystanders—to lend a hand in times of crisis.

Coping with terrorism requires localized, open, and inclusive engagement of civil society. But the U.S. government has neither adequately informed nor empowered civilians to play a meaningful role in defending the country. To better involve civilians in homeland security, the United States must remove the inadvertent obstacles it has placed in their way. Citizens, in turn, must be willing to grapple

with the risks they and their communities are likely to face and embrace a more active role in preparing for disasters.

DEVELOPING TRUST

To IMPROVE the nation's capacity to manage dangers, federal agencies must avoid alienating the very people they are responsible for protecting. Regrettably, Washington's growing homeland security bureaucracy has largely overlooked the need to garner support from the public. New security measures are advanced without spelling out the vulnerability that they are designed to address. The American public has generally tolerated this thus far, but presuming the public's submissiveness risks breeding resentment and lack of cooperation over time. Alternatively, when citizens understand the appropriateness of a given security measure, they will be more willing to collaborate to achieve its goal.

When the TSA introduced full-body X-ray scanners and enhanced pat-downs at U.S. airports last fall, it prioritized public compliance over public acceptance. Given the coercive tools at its disposal, the TSA correctly presumed that it could force civilian acquiescence to this more intrusive passenger screening process. But the marginal additional capabilities provided by the scanners and pat-downs came at a heavy cost. Public confusion and anger over the new program, expressed by the Thanksgiving holiday travel opt-out campaign, spawned a vocal minority that has sown general public skepticism and may impede future U.S. government efforts to improve homeland security.

In explaining its security measures to the public, the government should not promise more than it can deliver. U.S. officials should avoid making the kind of statements issued frequently after September 11 to the effect that terrorists have to be right only once, whereas U.S. officials have to be right 100 percent of the time. Such declarations might demonstrate firm resolve, but it sets an impossible standard; no security regime is foolproof. Common drug-smuggling techniques can evade the new scanning technology at U.S. airports. Radiation portal monitors, deployed with much fanfare at U.S. seaports, are unlikely to detect shielded nuclear material, raising the possibility that a nuclear weapon or dirty bomb encased in lead

could pass through undetected. Public officials should acknowledge the potential limits of these technologies and other security protocols in deterring terrorists. Creating unrealistic expectations guarantees anger, disappointment, and mistrust should a terrorist attack succeed.

U.S. policymakers should also refrain from measures that provide the optics of security rather than real security. For example, the presence of cement barriers outside a train station may reassure daily commuters. But if those barriers are not anchored to the ground, an explosive-laden truck could ram them aside and make it to the station's entrance. The ensuing tragedy would leave commuters feeling rightfully deceived and the families of victims outraged. Security protocols must survive a "morning-after test"; that is, they should be able to withstand a postmortem by the public about their adequacy, even if they failed to thwart an attack. If the post-incident assessment deems the security measures to be lacking credibility, there will be hell to pay.

OPEN UP

National security officials should also resist the secrecy reflex. U.S. intelligence and federal law enforcement agencies perform too much homeland security work behind closed doors. Their proclivity to operate in a world of restricted documents and windowless rooms often leaves both the private sector and the general public out of the loop.

On the surface, it seems sensible to avoid releasing information about vulnerabilities or security measures that potential adversaries could exploit. But this insularity often undermines the defense of critical infrastructure, such as seaports, dams, and waterworks. In determining the best way to protect a suspension bridge, for example, the bridge's chief engineer is likely to have ideas that would not occur to a law enforcement or military professional working in the Department of Homeland Security. But government officials frequently fail to consult that engineer. They will share security information only with vetted company security officers, who in turn are barred from passing this information on to senior executives and managers who do not

hold active security clearances. As a result, investment and operational decisions are often made with scant attention paid to the potential security stakes.

The U.S. government should increase its transparency with the broader public as well. Many policymakers believe that candor about potential dangers may generate excessive public fear. Yet the secrecy reflex often contributes to public anxiety. People are most frightened when they sense their vulnerability to threats but feel powerless to address them. U.S. officials have stated for nearly a decade that terrorism is a clear and present danger, but they have given citizens little information about how to cope with that hazard. Instead, citizens are told to proceed with their daily routines because the government is hard at work protecting them. The psychological effect of this is similar to that of a doctor telling a patient that she is suffering from a potentially life-threatening illness but providing only vague guidance about how to combat it. No one wants to receive disturbing news from his physician, but a prognosis becomes less stressful when doctors provide patients with all the details, a clear description of the available treatments, and the opportunity to make decisions that allow the patient to assert some personal control over the outcome. In the same way, the U.S. government can decrease fears of terrorism by giving the American public the information it needs to better withstand, rapidly recover from, and adapt to the next major terrorist attack.

Federal agencies must avoid alienating the very people they are responsible for protecting.

Flight attendants routinely tell passengers that they may need to use their seat cushions to stay afloat in the event of an emergency water landing. Although escaping a plane in the water is a frightening scenario, this safety instruction does not generate panic among passengers. Similarly, there is no reason why civilians should not be told what bombs and detonators look like, on the very remote chance that someone like the "Christmas Day bomber" ends up seated next to one of them on a plane. Having better-informed airport workers, flight crews, and passengers could prove a far more effective safeguard than deploying hundreds of new body scanners at airports.

AVOID OVERREACTING

WASHINGTON MUST also avoid overstating the threat of terrorism. Terrorist attacks are not all the same. Small-scale attacks of limited destructiveness pose the most likely terrorist danger to the United States today. Although Osama bin Laden remains on the loose, al Qaeda's senior leadership infrastructure has essentially been dismantled, undermining its ability to conduct sophisticated large-scale operations in North America. Aligned groups or other terrorist organizations may still organize catastrophic attacks, but such ambitious terrorist operations require groups of operatives with capable leaders, communications with those overseeing the planning, and time to conduct surveillance and to rehearse. Money, identity documents, and safe houses for operatives must be secured, and other logistical needs must be met. All this effort creates multiple opportunities for intelligence and law enforcement agents to disrupt plots before they come to fruition.

In the face of these challenges, terrorists have adapted their tactics. Now, attacks on U.S. soil are likely to be perpetrated by homegrown operatives who act alone or with one or two accomplices. Such operations are difficult to detect and intercept. Yet lone gunmen and suicide bombers can inflict only limited damage. Tragically, such attacks will destroy property and take innocent lives. But Mother Nature generates far more frequent and disastrous incidents. Virtually no terrorist scenario could equal the devastation caused by the March 2011 earthquake and tsunami that hit northern Japan. Similarly, it is hard to imagine that a terrorist armed with a weapon of mass destruction could produce more casualties than a global outbreak of a virulent strain of the flu virus: epidemiologists estimate that as many as 100 million people died of the Spanish flu in 1918. Even when terrorism is measured against other national security challenges, some perspective is warranted. During the height of the Cold War, a nuclear exchange with the Soviet Union would have left two-thirds of the American people dead and much of the world in ruins. That was a true existential danger, and one that the most ambitious terrorists cannot hope to match.

Similarly, U.S. policymakers must avoid overreacting to terrorist incidents when they do occur. In the aftermath of the bombing attempt aboard Northwest Airlines Flight 253, congressional leaders on both the left and the right declared it better to overreact than underreact to the risk of terrorism. This rare bipartisan consensus was unfortunately entirely wrong. Terrorism is fueled by the confidence that Americans will react to it by embracing draconian measures that damage the U.S. economy. Al Qaeda's October 2010 attempt to bomb airplanes by hiding explosives in ink cartridges shipped from Yemen was consistent with this strategy. The terrorists hoped that the midair destruction of any plane—cargo or civilian—would spur U.S. officials to respond with costly and disruptive methods that would undermine the movement of global cargo. In other words, their strategy depends on how Americans react—or, more precisely, overreact—to acts of terrorism.

Yet such smaller-scale, less destructive, and less lethal operations, even if unsuccessful, can produce this overreaction only when overwrought media coverage and political recriminations generate a rush to deploy expensive and often counterproductive new defenses. Conversely, a response of confident resilience to acts of terrorism would provide a real measure of deterrence by demonstrating that such attacks will not achieve their desired ends. Although the United States cannot prevent every act of terrorism, it can control how it responds to them.

THE WAY FORWARD

The U.S. government can avoid hindering its own actions to protect the homeland by building trust and setting proper expectations with civilians. To develop a comprehensive homeland security strategy, however, Washington should place greater emphasis on developing adequate societal resilience. Resilience is the capacity of individuals, communities, companies, and the government to withstand, respond to, adapt to, and recover from disasters. Since disruptions can come not just from terrorism but also from natural and accidental sources as well, advancing resilience translates into building a general level of preparedness. Ideally, a program of

resilience would address the most likely risks that people, cities, or enterprises may face. This would minimize the potential for complacency while assuring a level of basic skills, such as first aid and effective emergency communications, which are useful no matter the hazard.

Building societal resilience requires a bottom-up, open, and participatory process—that is, the exact inverse of the way U.S. policymakers have approached homeland security to date. A program of resilience mandates individuals, communities, and companies to take precautions within their respective areas of control. Success is measured by the continuity or rapid restoration of important systems, infrastructure, and societal values in the face of an attack or other danger.

Al Qaeda's strategy depends on how Americans react—or, more precisely, overreact—to acts of terrorism.

Resilience begins on the level of individuals. A program of resilience would promote self-reliance in the face of unexpected events, encouraging civilians to remain calm when the normal rhythms of life get interrupted. It would also teach individuals to make themselves aware of the risks that may confront them and to be resourceful by learning how to react to crises. And it would make preparedness a civic virtue by instructing civilians to refrain from requesting professional assistance unless absolutely necessary, thus freeing up manpower for those in the greatest need.

Promoting individual resilience involves acknowledging that many Americans have become increasingly complacent and helpless in the face of large-scale danger. Reversing this trend demands a special emphasis on educating young people. Students should learn to embrace preparedness as both a practical necessity and an opportunity to serve others. These students, in turn, can teach their parents information-age survival skills, such as texting, which may offer the only means to communicate when cellular networks are overloaded (800 text messages consume the same bandwidth as a one-minute call). As demonstrated in the aftermath of the 2010 Haitian earthquake and the Deepwater Horizon

oil spill that same year, social media are transforming the way rescuers and survivors respond to crises. These new tools have the power to turn traditional, top-down emergency management on its head.

Resilience also applies to communities. The U.S. government can promote resilience on the communal level by providing meaningful incentives for collaboration across the public, private, and nonprofit sectors before, during, and after disasters. Much like at the individual level of resilience, communities should aspire to cope with disasters without outside assistance to the greatest degree possible.

Building resilient communities requires providing community leaders with tools to measure and improve their preparedness based on a widely accepted standard. The Community and Regional Resilience Institute, a government-funded research program based at Tennessee's Oak Ridge National Laboratory, has spearheaded an attempt to define the parameters of resilience, modeled on the method by which fire and building codes were created and are maintained. It has drawn on a network of former governors and former and current mayors, emergency planners, and academics to develop detailed guidelines and comprehensive supporting resources that will allow communities to devise resilience plans tailored to their needs. Other countries, including Australia, Israel, and the United Kingdom, have instituted similar programs. Federal and state governments could provide communities that implement a comprehensive risk-awareness strategy and a broad-based engagement program with tangible financial rewards, such as reduced insurance premiums and improved bond ratings.

The tenth anniversary of September 11 will provide Obama with an opportunity to recalibrate the nation's approach to homeland security.

U.S. companies compose the third tier of resilience. Resilient companies should make business continuity a top priority in the face of a disaster. They should invest in contingency planning and employee training that allow them to serve and protect their customers under any circumstance. Corporations must also study the

capabilities of and partner with their suppliers and surrounding communities. Much like individuals and communities, corporations with resilience would possess the ability to sustain essential functions and quickly resume their operations at full capacity after a disaster. Resilience may also bring financial benefits to companies able to demonstrate their dependability in the wake of a major disruption. Such companies are likely to experience an increase in market share by maintaining regular customers and attracting new ones as well.

Although most large corporations invest in measures that improve resilience, smaller companies—which are the backbone of local economies and yet are constrained by limited resources—generally do not. But small businesses can rectify this in a low-cost manner by creating a buddy system between companies located in different regions. For instance, a furniture store in Gulfport, Mississippi, that may fall victim to an August hurricane could partner with a furniture store in Nashville, Tennessee, that may suffer from spring flooding. These businesses would agree to assist each other in providing backup support for data, personnel, customers, and suppliers in the event of a disaster.

INSTILLING RESILIENCE

To his credit, Obama explicitly identified resilience as a national security imperative in his May 2010 National Security Strategy. Homeland Security Secretary Janet Napolitano did the same in the February 2010 Quadrennial Homeland Security Review. Both have made frequent references to the importance of resilience in their speeches. But neither the federal bureaucracy nor the general public appears to be paying much attention.

The approaching tenth anniversary of September 11 will provide Obama with an opportunity to recalibrate the nation's approach to homeland security. While honoring the enormous sacrifice of the U.S. armed forces and those who have been working to protect the U.S. homeland, he should ask citizens to step forward and assume their own unique role. For individuals, families, neighbors, employers, and employees, the way to honor the lives so tragically lost in the

Twin Towers, in the Pentagon, and aboard United Airlines Flight 93 is to unite in preparing for future emergencies. The president should ask citizens from every walk of life to embrace a personal commitment to making the United States more resilient.

When passengers enter the new body scanners at U.S. airports, they are directed by TSA screeners to hold their hands above their heads and stand still while their images are taken. The position closely resembles the universal stance for surrendering—undoubtedly why many find the process so uncomfortable. An emphasis on resilience, by contrast, is consistent with the U.S. tradition of grit, determination, and hope in the face of adversity. When tested, Americans have always bounced back better and stronger. It is long past time for Washington to stop treating civil society as a child to be sheltered and to acknowledge the limits and counterproductive consequences of relying so heavily on protective measures. In good times and bad, the greatest asset of the United States has always been its people.