Amanda J. Dory

American Civil Security: The U.S. Public and Homeland Security

Has homeland security planning effectively prepared the U.S. public today for future terrorist attacks? The war on terrorism pursued abroad—the offensive component of homeland security—seeks to disrupt and defeat terrorists beyond U.S. borders. Yet, with officials at the highest level consistently sending the message that the threat of terrorism within U.S. borders is not going away anytime soon, it is time to create a common defense: a more resilient U.S. population that is better prepared to survive and cope with future attacks as well as their economic and psychological consequences here at home.

Since the September 11 attacks, the U.S. public has faced a new learning curve with each succeeding crisis—anthrax letters, sniper attacks, monkey pox, SARS, and power-grid failures—first trying to determine whether terrorism is involved in each instance and then how to deal with the problem at hand. Efforts to educate the public about the range of terrorist threats, our vulnerabilities to terrorism, and ways to respond during attacks have been limited, confusing, and at times even contradictory. This reflects the pursuit of other homeland security priorities; an intellectual debate on whether terrorism represents one hazard among many or a unique phenomenon; and diverging views as to whether the U.S. public needs to be reassured, scared into taking action, or a bit of both.

The stakes are too high to rely on a patchwork of cumulative learning from events still to come. Deficiencies in Americans' emergency preparedness have been made sufficiently apparent. Evacuation plans are lacking at every level, from families and businesses up through state governments. A

Amanda J. Dory was a 2002–2003 Council on Foreign Relations International Affairs Fellow at CSIS when she wrote this article. She is now working in the Homeland Defense Office within the Office of the Secretary of Defense.

The Washington Quarterly • 27:1 pp. 37–52.

comprehensive warning system does not exist by which to reach the public to provide guidance on what to do in an emergency. Individuals have little basis for making informed decisions in the face of an event involving chemical, biological, radiological, or nuclear (CBRN) effects. Procedures to undertake mass vaccinations or to distribute medical countermeasures have not been rehearsed. Perhaps most ominous, the U.S. public lacks confidence in information provided by authorities. As evidenced by the federal "Ready" campaign's devolution into a duct-tape frenzy that coincided with raising the homeland security threat level to orange for the first time in the spring of 2003, the public's capacity to absorb unfamiliar information in a stressful environment is not optimal. The communication of uncertain threats and equally uncertain response plans, combined with media treatment long on hype and short on science, breeds the kind of public fear and confusion that undermine the public's confidence in itself and in the U.S. government, thus furthering terrorists' goals.

Renewed attention to individual Americans and their contribution to and participation in domestic security might best be called "civil security," a term that harkens back to the Cold War U.S. civil defense effort but is firmly grounded in the current homeland security context. Civil security refers to measures undertaken to reduce the U.S. public's vulnerability to the physical, psychological, and economic impacts of terrorism as well as measures to enable individuals to minimize damage and recover from terrorist attacks in the United States. Civil security thus parallels the Bush administration's broad definition of homeland security[1] but with particular emphasis on the U.S. public. Civil security requires increased efforts by the full range of homeland security players: individuals must participate in civil security on their own behalf, while governments pursue it for their constituents and businesses address it with their employees. By enhancing individual understanding of terrorism's risks as well as effective, specific protective action responses, a comprehensive approach to civil security can further steel Americans against future terrorist attacks.

Why Civil Security?

In the inaugural National Strategy for Homeland Security, the Bush administration articulated a sweepingly inclusive vision of a partnership for homeland security: "The [a]dministration's approach to homeland security is based on the principles of shared responsibility and partnership with the Congress, state and local governments, the private sector, and the American people."[2] In considering the public's role in dealing with terrorism, however, decisionmakers tend to view American individuals not as partners but as ei-

ther potential attack victims or panicked masses. Rather than paying attention to individuals directly, government decisionmakers, often at the federal level, tend to view state and local governments and/or emergency responders as proxies for the people.

Increased government attention to the role of the public is crucial for a number of reasons. First, terrorist attacks target public confidence (in itself and in the government), individual American lives, and the American way of life more broadly. Americans risk becoming victims of future terrorist attacks, not only from possibly being in the wrong place at the wrong time but also from the economic and psychological fallout that would result from such attacks. As the September 11 attacks revealed, terrorism's reverberations reach far beyond the death toll, resulting in billions of dollars of economic loss and incalculable national distress. Because terrorism directly affects individuals and their livelihood, preparations to address the consequences of terrorism cannot be divorced from the very people these measures are ultimately intended to benefit.

Increased government attention to the role of the public is crucial.

Second, public support and cooperation are critical throughout any crisis both for emergency response and for long-term recovery. For example, the public's failure to comply with authorities' instructions to quarantine themselves in their homes or in a designated facility could prolong or worsen an incident involving contagious biological agents such as smallpox. Similarly, spontaneous evacuations in areas surrounding a radiological, or "dirty bomb," explosion could complicate authorities' decontamination efforts. On the other end of the evacuation spectrum, refusal to comply with directions to evacuate promptly could also endanger lives and hinder emergency responses. A recent study revealed that, if directed to do so, 90 percent of respondents nationwide would not comply with a directive to evacuate immediately during a crisis and would instead seek out additional information or otherwise prolong or avoid rapid departure.[3] Increasing the public's willingness and ability to respond appropriately to terrorist attacks and to return to normalcy thereafter is clearly in the interests of individuals, the private sector, and all levels of government alike.

Third, the U.S. population provides the financial resources needed for homeland security through tax dollars paid to federal, state, and local governments and through security costs that businesses pass on to consumers. Devoting these resources to homeland security, at an estimated cost of $100 billion annually,[4] results in very real and tangible trade-offs from other pri-

ority areas such as education, health, and Social Security benefits. Officials at all levels of government thus have to justify and build public support not only for decisions on how much domestic security is enough but also for the ensuing winners and losers in the resource allocation process.

Based on statements by national leaders, public participation in homeland security efforts clearly counts on a rhetorical level. In Atlanta in late 2001, in a major speech dealing with homeland security, President George W. Bush stated, "[W]e are a nation awakened to danger. … Our nation faces a threat to our freedoms and the stakes could not be higher. … This new era requires new responsibilities, both for the government and for our people."[5] Similarly, Secretary of Homeland Security Tom Ridge referred to the U.S. citizen as "the ultimate stakeholder" and the need to "empower citizens to play a more direct role" in homeland security.[6] To date, these new roles and responsibilities for the people have yet to be articulated in detail, allowing the misperception that governments are exclusively charged with maintaining homeland security to continue.

Lessons Learned from Civil Defense

A historical precedent for educating and involving the U.S. public directly in homeland defense efforts can be found in civil defense measures taken during the Cold War. From the early 1950s until 1994, when Congress pulled the plug on the program at the end of the Cold War, civil defense comprised a variety of programs including public shelters, stockpiles of supplies, radiological detection devices, education, training, warning systems, and so forth. The goal of Cold War civil defense was to enable the greatest number of Americans to survive a Soviet nuclear attack on the United States should one occur. Through outreach and educational activities, the government provided the public with a basic understanding of the nature of the Soviet threat, the nation's vulnerability to nuclear attack, and potential consequences if one were to occur. Certain aspects of the civil defense program were quite sound, including its comprehensiveness, voluntary nature, strong focus on education, distribution of costs throughout society (to federal, state, and local governments and to individuals), and patriotic linkage to a larger sense of community and civic duty.

Civil defense was not without flaws, however. Resources for the civil defense program waxed and waned over time, and its focus shifted significantly to reflect the changing threat environment as well as the views of the U.S. executive and legislative leadership on how to deter the Soviet Union using a combination of offensive (strategic nuclear forces) and defensive (civil defense) measures. Late in the Kennedy administration, the shift to a doctrine

of mutually assured destruction, premised on the ability to inflict horrendous losses on civilian populations, undercut the strategic rationale for a civil defense program designed to protect the public—a discontinuity that continued for two decades. As for the public itself—ostensibly the most important constituency the program was designed to serve—the vast majority of the U.S. population did little or nothing, responding to civil defense with a mixture of indifference, fear, anger, and occasional support. Some believed that nothing useful could be accomplished, while others were in denial and failed to acknowledge the threat; still others considered a program that might not save all people to be immoral. Thus, civil defense failed to attract the enduring public interest and support necessary to realize the goal of a nation prepared to survive a Soviet nuclear attack.

A historical precedent can be found in civil defense measures taken during the Cold War.

Unfortunately, in the collective consciousness, memories of civil defense have been boiled down to a duck-and-cover bumper sticker, tinged with ridicule, rather than a more balanced assessment. As former senators Gary Hart (D-Colo.) and Warren Rudman (R-N.H.) stated in a recent task force report, "The contemporary security environment mandates that we put this anti–civil defense bias behind us."[7] Although imperfect, the Cold War civil defense program nonetheless had a clear focus on the people as a strategic national resource and on the necessity and desirability of their participation to promote domestic security.

A Modest Proposal: Civil Security

A comprehensive and updated effort comparable to that employed by the United States in the face of the Soviet threat has yet to emerge in today's threat environment, in which attacks on U.S. soil have already occurred and future ones are anticipated. Based on lessons from Cold War civil defense, several characteristics of a program designed to increase the U.S. public's resilience and ability to cope with terrorist attacks today are apparent. They include:

- *effectiveness*, or the capability to save lives;
- *flexibility*, or a capacity to evolve in tandem with changes in the security environment;
- *inclusiveness*, or the ability to address a tremendously diverse U.S. population;

- *comprehensiveness*, or an expansive conception that accounts for the public before, during, and after terrorist incidents; and

- *affordability*, or a burden-sharing arrangement that distributes and rationalizes costs among stakeholders in homeland security.

An underlying tension within the emerging homeland security field of expertise is the extent to which terrorism and the responses it requires are distinct from other man-made and natural disasters. The debate can be grossly simplified by dividing it into two camps that roughly correspond to the national security community, which tends to focus on the uniqueness of deliberate terrorist attacks relative to accidents and natural phenomena, and the disaster response community, which emphasizes the similarity of responses (for example, roles played by emergency managers and first responders) across the full range of hazards, referred to as "all hazards" by practitioners.

Does terrorism require responses distinct from other man-made and natural disasters?

Three aspects of terrorism make it difficult to add terrorism neatly into the all-hazards spectrum of disasters. First, through the deliberate use of CBRN effects, terrorist attacks have the potential to increase significantly the casualty levels historically associated with other types of disasters and accidents. Second, as adaptive adversaries, terrorists not only have the ability to change tactics as an attack unfolds but also can "reload" rapidly[8] and/or pursue multiple attacks simultaneously—characteristics that do not apply to natural hazards and accidents. Third, terrorist attacks are criminal acts and, as such, include the additional complications of securing a crime scene and conducting an investigation during the response phase. Although the debate may seem arcane at first glance, it directly influences how the government encourages the public to think about terrorism and prepare for terrorist attacks, that is, whether terrorism is just another disaster or whether it requires unique treatment.

An effective civil security effort should split the difference, so to speak, by building on the all-hazards foundation, recognizing that aspects of emergency response are indeed applicable across the board, yet elements particular to terrorism require distinct protective actions as well as specialized preparations. The chart in figure 1 summarizes how needed detection capabilities, protective actions, and protective equipment can differ depending on whether an incident is conventional (involving explosives alone) or has CBRN effects.

A "one size fits all" response to terrorist attacks is misleading and potentially dangerous in a dynamic, complex, and scenario-dependent threat environment. An effective civil security approach would entail informing the public as to which responses are the most effective against which threats and in what circumstances specialized preparedness items may be required. For example, Americans need to understand that sealing windows and doors with duct tape and plastic is a useful protective action only in specific situations, such as attacks involving chemical effects, and must be followed promptly by venting the affected area after contaminated external air has dissipated. Similarly, particulate masks can provide limited protection in situations involving radioactive dust, certain viruses (depending on size), and aerosolized chemical agents, but they are useless against chemical vapors. Meanwhile, biological incidents are fundamentally different from other attacks because the effects evolve gradually and are not immediately detectable. A one-size-fits-all preparedness campaign and checklist obscures these important distinctions; a far-reaching educational campaign is the only way that individuals will be able to grasp these differences.

To address the role of the U.S. public in homeland security before, during, and after terrorist attacks, at least four key components are needed in a contemporary civil security approach: risk education, preparedness, warning, and protective actions. These same components all have some precedent in the Cold War civil defense program but obviously require retooling for a new set of adversaries with an expanded arsenal of weapons of mass destruction.

Risk education refers to an interrelated approach to encourage Americans to play an active and supportive role in defense against terrorism: the processes of risk assessment (assessing threats and vulnerabilities in an integrated way), risk psychology (how people think about terrorism), and risk communication (adapting information to how people learn best about risk). Inspiring public support requires a realistic portrayal of risk that is accurate and draws a fine line between hyping the threat to spur people to action and trivializing it to provide them false reassurances. Risk education provides the foundation of civil security and is a fundamental prerequisite to enable individuals to minimize damage and recover from terrorist attacks. It can provide the impetus for Americans to undertake voluntary emergency preparedness activities. It can also serve as the basis for individuals to make informed decisions during an emergency and take protective actions expediently if official warnings with recommended actions are not immediately available.

Preparedness provides a way for individuals, communities, and institutions to translate risk awareness into action. Preparedness can consist of a range

Figure I: Terrorist Attacks and Individual Protective Actions

Types of Attack	*Detection Capability*	*Short-Term Protective Action(s)*	*Individual Protective Equipment*[2]	*Medium-Term Response*	*Related Historical Experience*
CONVENTIONAL					
• Delivery: vehicle, plane, suicide bomber, building attack	• Explosive-sniffing dogs • Explosion	• N/A • Medical care for victims	• N/A	• Recovery and reconstruction	• U.S.: Sept. 11, 2001; Oklahoma City bombing (1995)
CHEMICAL					
• Types: blister agents, nerve agents, pulmonary agents • Delivery: airborne (aerosol, vapor), food-borne, or waterborne; attack on chemical facility or transit	• Limited sensor detection capability deployed[1] • Explosion • Victims evident or present for medical care	• Some medical countermeasures • Decontamination for immediately exposed individuals • Expedient shelter-in-place for several hours (duct tape, sheeting), then venting • Evacuate (from downwind areas if time available)	• Expedient: N95 or P100 particulate masks • Specialized: escape hoods, chemical respirators, protective clothing and hoods	• Venting buildings and homes for airborne agents • Decontamination of surfaces and buildings for persistent agents[3]	• U.S.: Baltimore, Md., chlorine train accident (2001) • World: Mississauga, Canada (1979); Bhopal, India (1984); Tokyo, Japan (1995)
BIOLOGICAL					
• Types: bacteria (e.g., anthrax), virus (e.g., smallpox), toxins (e.g., ricin)	• Epidemiological monitoring • Limited sensor detection capability deployed[1]	• Medical countermeasures (e.g., vaccination, antibiotics) for affected individuals • Mass vaccination	• Expedient: N95 or P100 particulate masks	• Decontamination of surfaces and buildings[3]	• U.S.: New York City smallpox epidemic (1947), Oregon salmonella poisoning (1984), anthrax mail attack (2001)

• Delivery: airborne, food-borne, or waterborne; human or animal transmission	• Anthrax detection at several postal facilities • Victims present for medical care	• Voluntary quarantine in home (shielding) in outbreak area • Government-directed quarantine for particular area	• Specialized: escape hoods, protective clothing and hoods	• Vaccination to prevent future outbreaks	• World: Sverdlosk, Soviet Union, anthrax (1979)
RADIOLOGICAL ('DIRTY BOMB')					
• Effects: blast, radioactive contamination • Delivery: bomb, food-borne or waterborne	• Radiation detection devices at transit points and other locations • Explosion • Victims present for medical care	• Decontamination for immediately exposed individuals	• Expedient: N95 or P100 particulate masks • Specialized: Protective suits for nuclear industry workers	• Decontamination of surfaces and buildings[3]	• World: Goiania, Brazil, cesium poisoning (1987)
NUCLEAR					
• Effects: blast/initial radiation, electromagnetic pulse (EMP); fallout • Delivery: nuclear device, ballistic or cruise missile, attack on nuclear power plant	• Explosion • Disruption of electronic devices by EMP • Radiation detection devices	• Shelter-in-place, preferably underground (days or longer—depends on proximity to attack location) • Evacuate (from downwind areas if time available) • Potassium iodide to protect thyroid • Decontamination of affected individuals	• Specialized: Protective suits for nuclear industry workers	• Long-term evacuation from affected areas • Medical monitoring for individuals • Decontamination of surfaces and buildings may not be possible	• U.S.: Three Mile Island, N.Y. (1979) • World: Hiroshima and Nagasaki, Japan (1945); Chernobyl, Soviet Union (1986)

1. The Department of Homeland Security Biowatch program has a limited detection capability in some 30 unspecified locations, while the Department of Defense has a parallel detection system at some 200 U.S. installations. The national laboratories and at least one specialized National Guard team are also involved in pilot detection efforts.

2. In many cases, specialized equipment is available to industrial workers and the military but not the general public.

3. May or may not be economically feasible depending on the agent and extent of contamination.

of activities, including developing and practicing contingency plans (such as communication, evacuation, or sheltering), participating in education and awareness activities, providing first aid and emergency response training, and stockpiling emergency supplies. Preparedness serves as a bridge between risk education (which occurs in advance of an event) and taking protective actions during a crisis. Preparedness for all hazards (such as stockpiling three days' worth of food and water) may be applicable and useful during a crisis triggered by a terrorist attack. There are several preparedness items that are not all-hazards in nature, however, including respiratory protection, duct tape and plastic, and certain kinds of medical countermeasures. These would only be relevant for attacks (or accidents) involving CBRN effects.

A 'one size fits all' response to terrorist attacks is misleading and potentially dangerous.

Warning aims to save lives and to reduce the costs of disasters by giving guidance on specific actions to take in a crisis. In contrast to risk education, federal, state, and local government officials issue warnings with urgency in a crisis environment via predominantly privately operated communications channels (such as television, radio, telephone, and wireless devices). Unlike the advance notice of an escalating crisis that likely would have preceded a Soviet attack during the Cold War, terrorist attacks are designed to surprise; thus, warnings are more likely to be issued during and immediately following a terrorist incident rather than in advance. Precisely because official guidance may not be immediately available during an attack or its immediate aftermath, individuals must be empowered with the knowledge and capacity to make their own decisions on the spot.

Protective actions consist of steps that individuals and communities can take to save lives and to reduce losses when an event occurs. The ultimate test of civil security is the effectiveness of protective actions, that is, what people actually do in a crisis. Examples of protective actions include different forms of sheltering, evacuation, and quarantine (voluntary or mandatory); using individual protective equipment such as respiratory equipment or protective clothing; and using a variety of medical countermeasures including vaccines, antidotes, antibiotics, and potassium iodide. Risk education, preparedness, and warning are all intended to improve the public's knowledge and its ability to respond in ways that reduce loss of life during a terrorist attack through effective protective actions. The chances for successful protective actions can also be increased through the existence of plans for how the actions are to be executed and advance communication of

the content of such plans to potentially affected parties (notably the public) to build understanding and confidence. Figure 1 shows when different protective actions would be relevant for CBRN terrorist attacks, underscoring that a standardized approach does not work for the range of potential scenarios.

Collectively, these four interactive elements can reinforce one another as part of a comprehensive civil security approach that focuses on the U.S. public under the larger homeland security umbrella.[9] As described, civil security components provide the tools to maximize the odds for physical survival of a terrorist attack. They can also serve to mitigate the psychological and economic consequences of terrorist threats or acts. Household and business preparedness activities, for example, can provide reassurance in addition to their practical value. Similarly, warnings that are targeted for specific populations at risk can avoid unnecessarily dampening economic activity in areas where precautions are unwarranted.

Making It Work

Creating a civil security focus within current homeland security efforts is not a herculean undertaking. What it does require is a clear sponsor within the federal structure, a modicum of funding, sustained attention, and participation by all stakeholders in homeland security. A quintessential lesson learned from the experience of Cold War civil defense is that bureaucratic success requires a dedicated and identifiable sponsor with assured access to senior government officials. To advance civil security concerns in the short term, the most effective structural solution would be the creation of a small civil security liaison office within the immediate office of the secretary of homeland security. This office would join counterparts in the front office that have been created for the other homeland security stakeholders, including a special assistant for the private sector, a legislative affairs office, and an office responsible for state and local government coordination. There is also current debate about moving the Office of Domestic Preparedness (formerly part of the Department of Justice) that liaises with the emergency responder community to be a component of the secretary's office.

Although the Department of Homeland Security (DHS) already has an Office of Public Affairs, it primarily uses media channels to represent the work of the entire department and of its key officials; the office is not designed to be a two-way conduit for risk education. Communications skills are critical for a civil security program, but they need to be buttressed by additional technical knowledge and a mandate for coordination across the DHS organization (and also with other agencies) to address issues relating to risk education, preparedness, warning, and protective actions in an inte-

grated way. The term "liaison office" is used deliberately to underscore the two-way communication with the U.S. public that is needed for civil security, much the way that the current DHS office that deals with state and local issues serves as a liaison.

The work of the civil security liaison office should be twofold. First and foremost, the office must be charged with connecting the dots, that is, developing linkages among diverse activities that have direct impact on the entire U.S. population so that, from the public's perspective, a coherent game plan is provided to instruct people how to respond to a terrorist attack and how their capabilities will be buttressed by governmental resources. Second, in terms of philosophical approach, the liaison office should acknowledge the merits of the all-hazards approach as a foundation but at the same time take responsibility for making clear to the public which types of preparedness activities and protective actions are relevant for different kinds of terrorist attacks, particularly for each of the CBRN constituent parts (chemical, biological, radiological, and nuclear). An added benefit of this all-hazards "plus" approach is that it can allow changes in emphasis in the future as the nature of the threat evolves. In periods when the threat recedes, preparedness for a terrorist attack can be deemphasized relative to other hazards (i.e., natural disasters) and vice versa, thus providing programmatic flexibility and sustainability over time.

Four existing federal efforts under the purview of DHS are logical pillars that can support a civil security program: the Ready terrorism preparedness campaign, the Citizens Corps initiative, the Emergency Alert System (EAS), and the Strategic National Stockpile (SNS). They are currently managed by different parts of DHS and the Centers for Disease Control and Prevention (CDC) with little vision of how they interrelate from the public's perspective. The civil security liaison office could provide that vision without necessarily assuming operational responsibility for all of the programs.

The Ready campaign initiative debuted in March 2003 and comprises a Web site, public service announcements, and a toll-free information number. The Web site is off to a good start, with 15.5 million unique page views. In addition, the toll-free telephone number that callers can use to request an informational brochure has received 130,000 calls.[10] With a U.S. population of 290 million, however, a great deal more remains to be done, especially for those without Internet access. Launched as a result of a private foundation grant (with close to $3 million in start-up funds provided by the Sloan Foundation), federal funding is now required to sustain the campaign over time to ensure the continued expansion of risk awareness and preparedness among the U.S. population. Current and future administrations, as well as Congress, must ensure that the campaign receives adequate resources to reach more Americans,

to fine-tune its messages, and to measure its effectiveness through surveys and focus groups on a continuing basis. Short-term priorities include translation of Ready content into multiple languages, the addition of specific CBRN scenarios (historical and hypothetical) to the Web site to improve individuals' understanding of how terrorist attacks could potentially unfold, and interactive functionality to allow two-way dialogue with the public. To reach a greater number of Americans, DHS must also focus on reaching people in nontraditional ways, including making use of such locations as grocery stores, banks, gas stations, and other facilities that most people have to visit in the course of their daily lives.

The ultimate test of civil security is the effectiveness of protective actions.

The second existing program, the Citizens Corps initiative, is an umbrella structure with distinct community-based functions: fostering volunteer service, which regroups well-known existing programs such as Neighborhood Watch and Community Emergency Response Training, and facilitating education and outreach. The latter involves establishing a new structure altogether—Citizens Corps Councils—at state and local levels. These councils mirror similar efforts used to mobilize and reach Americans during the Cold War civil defense days. In a short period of time, the Citizens Corps initiative has managed to attract a healthy number of federal and nonfederal partners[11] that share the goal of helping communities prevent, prepare for, and respond to disasters. To date, 50 state and territory councils and 770 local councils have been formed.[12] These councils, with a grassroots flavor that can give them relevance and credibility within local communities, can serve as two-way conduits in the risk education and risk communication process. For the program to succeed, however, administrations must propose and Congress must approve the nominal funding required over time to supplement and sustain the organizational capabilities and human resources provided by dedicated local volunteers and the educational and training activities they sponsor in the community. Unfortunately, the initiative did not receive congressional funding for fiscal year 2003, despite the administration's request for $100 million. For FY 2004, the administration requested $181 million; in September 2003, Congress approved $40 million.

The third existing building block for a civil security program is the EAS, a leftover warning system from Cold War civil defense days that provides warnings via radio and television. The EAS is jointly managed by the Federal Emergency Management Administration (now located within DHS), the National Oceanographic and Atmospheric Administration (NOAA)

(NOAA Weather Radio is a key channel for warnings), and the Federal Communications Commission. The lack of complete ownership by any single entity, however, has produced both bureaucratic inertia and friction over time. In addition, the EAS urgently needs updating to accommodate and incorporate the proliferation of communications devices and media beyond traditional television and radio outlets. On the receiving end, individual Americans need to think about how warnings can reach them 24 hours a day, seven days a week (even in the event of a power outage) and acquire appropriate devices to receive such warnings. Even so, it is possible or even likely that, in the early minutes and hours following a future terrorist attack, the U.S. public will have to respond as best as possible on its own, without immediate access to considered advice from local, state, or federal officials. This situation underscores the need for better risk education up front so that individuals are equipped with information that can improve their ability to survive.

The American people need a clear advocate at the federal level.

For protective actions, the SNS, an essential source of specialized CBRN medical countermeasures, is truly a national treasure. Managed for DHS by the CDC, the SNS provides capabilities and supplies that can be deployed on short notice to assist state governments if requested. SNS "push packages" contain antibiotics, vaccines, and other medical supplies and are located in multiple undisclosed locations across the country. Materials in the SNS must continue to be expanded based on evolving threat information. Countermeasures developed for military use must also be explored for their civilian relevance and potential inclusion in the SNS. Beyond the existence of the stockpile, developing state, community, and individual plans is indispensable to execute protective actions such as evacuation, sheltering inside or outside the home, and quarantine successfully. Public understanding of the plans in which they will be involved is also essential and can be conveyed as part of the risk education process. The current effort to update and expand the Federal Response Plan, which lays out roles for federal agencies in disasters of all kinds, to make it a National Response Plan involving stakeholders beyond the federal level, provides an opportunity for state and local governments to develop and/or update protective action plans.[13] Such plans then need to be communicated to members of the public so that they are not revealed for the first time in a crisis situation when anxieties and the potential for miscommunication are high.

Building Mutual Government and Public Trust

The American people need a clear advocate at the federal level who will focus on their interests before and throughout a terrorist attack, in contrast to activities such as critical infrastructure protection, port security, and border security that benefit Americans but do not directly involve them for the most part. Public opinion surveys since September 11, 2001, consistently show that a significant portion of the U.S. population is concerned about terrorism. According to an August 2003 survey, 76 percent of the respondents were concerned about the possible occurrence of additional terrorist attacks; the figure was even higher in New York City.[14] This level of concern was matched by a strong sense of community and a desire to help in local emergency planning. Yet, new initiatives such as the Ready campaign and the Citizens Corps are still largely unknown to the U.S. public, and few individuals, families, and communities have developed recommended emergency plans. For example, the Columbia University survey found that only 23 percent of respondents had a basic emergency plan and supplies, while a DHS-sponsored survey showed that 20 percent considered themselves prepared for a terrorist event.[15]

The civil security approach proposed here seeks to bridge two gaps: the gap between idle concern and useful action by Americans and the gap between rhetoric about the importance of the citizen stakeholder in homeland security and the tangible results to date. Efforts to improve risk education, preparedness, warning, and protective actions and to recognize the linkages between these components can strengthen the ability and resolve of individuals, neighborhoods, and communities to endure and prevail against adversaries who deliberately seek to instill fear and undermine Americans' confidence in themselves and in their government. Civil security also provides an outlet for individual participation in and contribution to homeland security. Several existing programs described here can serve as building blocks for a civil security program. If linked together conceptually and adequately funded, these measures could improve the population's resilience and ability to respond in the event of future terrorist attacks on the United States.

About 40 years ago, at the height of the Berlin crisis, President John F. Kennedy declared, "To recognize the possibilities of nuclear war in the missile age, without our citizens knowing what they should do and where they should go if bombs begin to fall, would be a failure of responsibility."[16] Today's stakeholders in homeland security—federal, state, and local governments; the private sector; individuals; and communities—must collectively face up to this responsibility as well. Such an effort will require clear vision and strong leadership in two directions, from the federal level down and from individual Americans up, to create a more resilient population in the face of terrorist adversaries with intentions to inflict widespread harm.

Notes

1. The Bush administration defines homeland security as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage from attacks that do occur." Office of Homeland Security (OHS), "National Strategy for Homeland Security," July 2002, p. 2, www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf (accessed October 2, 2003).
2. Ibid.
3. National Center for Disaster Preparedness, Mailman School of Public Health, Columbia University, "How Americans Feel About Terrorism and Security: Two Years After 9/11," August 2003, p. 10, www.ncdp.mailman.columbia.edu/How_Americans_Feel_About_Terrorism.pdf (accessed October 2, 2003) (hereinafter terrorism survey).
4. OHS, "National Strategy for Homeland Security," p. xii.
5. "This New Era Requires New Responsibilities," *Washington Post*, November 9, 2001, p. A15 (transcript of speech by President George W. Bush).
6. Tom Ridge, remarks at "Homeland Security from the Citizen's Perspective" meeting, Council on Excellence in Government, Washington, D.C., September 16, 2003.
7. Gary Hart and Warren B. Rudman, *America Still Unprepared—America Still in Danger* (New York: Council on Foreign Relations, 2002), p. 16, www.cfr.org/pdf/Homeland_Security_TF.pdf (accessed October 2, 2003) (report of an independent task force).
8. For a discussion of the reload phenomenon, see Richard Danzig, *Catastrophic Bioterrorism: What Is to Be Done?* (Washington, D.C.: National Defense University Press, January 2003), sec. 1.
9. See Amanda Dory, *Civil Security: Americans and the Challenge of Homeland Security* (Washington, D.C.: CSIS, 2003), www.csis.org/isp/civilsecurity.pdf (accessed October 29, 2003).
10. Office of Public Affairs, Department of Homeland Security (DHS), communication with author, Washington, D.C., June 2, 2003.
11. At the July 2003 National Citizens Corps conference in Washington, D.C., the National Oceanographic and Atmospheric Administration, the Environmental Protection Agency, and the Department of Education signed on as new federal partners, with the Departments of Homeland Security, Health and Human Services, and Justice established as charter partners. Nonfederal affiliate programs involved nine organizations, including the American Red Cross, Jaycees, and the Points of Light Foundation.
12. Office of Citizens Corps, DHS, communication with author, Washington, D.C., September 29, 2003.
13. Office of the Press Secretary, The White House, "Homeland Security Presidential Directive/HSPD-5," February 2003, www.whitehouse.gov/news/releases/2003/02/20030228-9.html (accessed October 2, 2003).
14. Terrorism survey. Other surveys have been done by Harvard University's School of Public Health, DHS, and the Gallup organization.
15. Terrorism survey; ORC Communications survey commissioned by DHS and presented at National Citizens Corps conference, Washington, D.C., July 2003.
16. John F. Kennedy, "Radio and Television Report to the American People on the Berlin Crisis," Washington, D.C., July 25, 1961, www.cs.umb.edu/jfklibrary/jfk_berlin_crisis_speech.html (accessed October 2, 2003).