Backgrounder

Published by The Heritage Foundation

No. 2150
June 24, 2008

Resiliency and Public–Private Partnerships to Enhance Homeland Security

James Jay Carafano, Ph.D.

The norm in international security affairs regarding homeland security is characterized by distrust and bitter debate (such as the United States' four-year confrontation with Europe over negotiating how to share Passenger Name Record data for international air travel) or wrong-headed national programs that ignore the realities of global commerce (such as the U.S. requirement for 100 percent screening of inbound container cargo). Addressing these shortfalls requires shifting from unrealistic strategies that emphasize protecting infrastructure to strategies that focus on the concept of resiliency.

"Strategies of resiliency" means methods for making sure that basic structures and systems of global, national, and local economies remain strong even after natural disasters or terrorist attacks. Fundamentally, in the context of terrorism, building a more resilient society is an effort to prevent and deter.

Strengthening most critical components of infrastructure or essential systems prevents terrorists from exploiting a society's vulnerabilities and dealing blows that could cripple it. Decentralizing and reducing the brittleness of necessary global and national systems demonstrates to terrorists the futility of attacking those systems—and thus deters.

This paper describes a model for building resiliency into public–private partnerships. The model is highly adaptable for sovereign nations, accommodating their cultures, laws, and practices. It also is a model for strengthening cooperation among free states and developing a broader global initiative on homeland

Talking Points

- The United States government must shift from unrealistic strategies that emphasize protecting infrastructure to strategies that focus on resiliency. Spending billions to protect infrastructure still leaves the nation vulnerable. Resiliency promises to sustain society in the face of known threats and unexpected disasters.
- A strategy of resiliency means making sure that the basic structures and systems of global, national, and local economies remain strong and can continue, even in the face of natural disasters or terrorist attacks.
- At its core, resiliency is a strategy that is national in character but international in scope.
- The U.S. government should promote public-private risk-management models by defining reasonable roles for government and industry, encouraging bilateral cooperation on liability issues, developing national and international forums for collaboration on resiliency issues, and promoting the development of resilient 21st century public infrastructure.

This paper, in its entirety, can be found at:
www.heritage.org/Research/HomelandDefense/bg2150.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies of the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

security that both respects national sovereignty and encourages international collaboration.

Congress and the Administration ought to make it easier for the U.S. government, state and local jurisdictions, and America's allies to adopt strategies of resiliency. Specifically, they should promote this approach by:

- **Establishing** improved public–private models for risk management that define reasonable roles for government and industry,
- **Encouraging** bilateral cooperation to address liability issues,
- **Developing** national and international forums for increasing collaboration, and
- **Innovating** to pave the way for resilient public infrastructure in the 21st century.

What Is Resiliency?

Resiliency, in the context of national security, is the capacity to maintain continuity of activities even in the face of threats, disaster, and adversity. The White House's 2007 *National Strategy for Homeland Security* concludes:

> We will not be able to deter all terrorist threats, and it is impossible to deter or prevent natural catastrophes. We can, however, mitigate the Nation's vulnerability to acts of terrorism, other man-made threats, and natural disasters by ensuring the structural and operational resilience of our critical infrastructure….[1]

The White House strategy goes on to explain:

> [W]e must collectively work to ensure the ability of power, communications, and other life-sustaining systems to survive an attack by terrorists, a natural disaster, and other assessed risks or hazards. In the past, investments in redundant and duplicative infrastructure were used to achieve this objective. We must now focus on the resilience of the system as a whole—an approach that centers on investments that make the system better able to absorb the impact of an event without losing the capacity to function. While this might include the building of redundant assets, resilience often is attained through the dispersal of key functions across multiple service providers and flexible supply chains and related systems. Resilience also includes the protection and physical survivability of key national assets and structures.[2]

Although the White House strategy focuses principally on physical infrastructure, policymakers should broaden strategies of resiliency to include all aspects of civil society from the local level to the international level. Building resilient communities, for example, should be the centerpiece of local preparedness and response programs.[3]

Why Resiliency?

Although resiliency offers some degree of confidence in sustaining material or physical systems, the decisive advantage is its psychological influence on civil society. In the end, the material impact of the concept of resiliency makes societies truly resilient in adversity. The most resilient societies are the ones that *believe* they are resilient.

World War II offers some prime examples.[4] The major combatants whose domestic populations underwent terrible suffering proved remarkably resilient even though all of these nations made minimal material preparations for conflicts that would ravage their homelands. Interestingly, each took a different path to get there.

The English, for example, showed their resilience during the bombings that set London afire,

1. The White House, Homeland Security Council, *National Strategy for Homeland Security*, October 2007, p. 35, at *http://www.whitehouse.gov/infocus/homeland/nshs/NSHS.pdf* (June 23, 2008).
2. *Ibid.*, p. 36.
3. James Jay Carafano, Jennifer A. Marshall, and Lauren Calco Hammond, "Grassroots Disaster Response: Harnessing the Capacities of Communities," Heritage Foundation *Backgrounder* No. 2094, December 28, 2007, at *http://www.heritage.org/Research/NationalSecurity/bg2094.cfm*.
4. Gerhard L. Weinberg, *A World at Arms: A Global History of World War II* (Cambridge, U.K.: Cambridge University Press, 2005).

drove residents underground each night, and forced parents to evacuate children to the countryside. Without question, American aid under the Lend-Lease Act and the entry of the Soviet Union and the United States into the war made all the difference in the ultimate defeat of the Axis powers. Nevertheless, even before the rush of U.S. aid, the British demonstrated a remarkable capacity to sustain the war effort, maintain a healthy civil society, and meet basic needs of their citizens.

Germany proved notably resilient as well. Rather than relying on the corporate spirit of the citizenry, however, the German model matched a highly centralized military planning system with enslavement of most of Western Europe. It was a brutal and vicious system, but it kept Germans armed and fed during a two-front war. Even at the height of Allied strategic bombing campaigns that leveled cities, German war production continued apace. The Soviet Union followed a mixed model, as elements of German totalitarian brutality combined with a stalwart nationalism that was the equal of Britain's.

National Will. All three societies—the British, the Germans, and the Russians—had vast resources at their disposal during World War II, but that hardly made them resilient. None had efficient plans for harnessing itself for global war. None was prepared for the unexpected ravages of strategic conflict that disrupted services, displaced populations, and burned vital infrastructure to the ground.

The British, the Germans, and the Russians proved resilient because they summoned the will to prevail and persevere through hardship; the acumen to organize delivery of needed goods and services; and the wherewithal to maintain an organized civil structure (albeit, in the case of Germany and Russia, despicable and horrific excuses for sovereign powers). Keeping the heartbeat of the nation going amid adversity is the very definition of resiliency, and national will is the key element in accomplishing this goal.

Napoleon, the French military genius who nearly conquered all of Europe in the 19th century, famously declared that in war, "the moral is to the physical as three is to one." This maxim holds true for thinking about the resiliency of the home front as well—in war and in peace, in the face of concerted enemies, unthinking natural disasters, and unintended man-made catastrophes.

Why Now? World War II should not be taken as an object lesson. It is a bad idea to wait until catastrophe strikes to discover how resilient your state can be. Complacency is a bad response, for two reasons.

The first is humanitarian. Although a society may demonstrate resiliency in recovering from disaster, much of its population and national treasure may be lost in the process. America proved resilient during the influenza pandemic of 1918 but failed to meet the challenge effectively. That failure cost 300,000 lives in the U.S. and millions more around the world when Washington's poor policies helped to spread disease. Thus, resiliency should be, first and foremost, a humanitarian undertaking that protects innocents from the ravages of natural and man-made threats.[5]

The second is legitimacy. Sovereign nations that fail to appear effective at the onset of a threat or crisis may lose legitimacy quickly. Contrary to popular misconception, panic is the exception rather than the rule. However, if the public does not believe its government is responding appropriately, that government may lose legitimacy in short order. This in turn may lead to increased anxiety, panic, and other forms of destructive behavior that undermine the stability of civil society.

In crisis, many individuals and communities take responsibility for addressing their own needs. Confidence in the resiliency of civil society further encourages them to assume responsibility themselves. The credibility of *governance* often is more important than specific actions of the *government*. Thus, the more credible the government response, the less the government actually is required to do.[6]

Resiliency as Strategy

At its core, resiliency is a strategy. When a government chooses resiliency, it makes a conscious decision

5. James Jay Carafano and Richard Weitz, eds., *Mismanaging Mayhem: How Washington Responds to Crisis* (Westport, Conn.: Praeger, 2008), Chapter 1.

about how to address future challenges. Resiliency as a strategy must be national in character. Homeland security is a national enterprise and as such must reflect the realities of a country's geography, culture, economy, politics, and other societal factors that make sovereign nations unique and distinct.

Strategies must be national in character but also international in scope. Nearly every homeland security program—from managing movement of goods, people, services, and ideas to controlling a border to investigating terrorist groups—requires international cooperation. This dimension of safeguarding the home front is nowhere more important than in addressing national infrastructure, supply-chain issues, and public–private partnerships. America is part of a global marketplace with a global industrial base. Virtually no nation is self-sufficient.[7]

Implementing resiliency requires a global perspective, which is no easy task. Still, it represents a superior strategy—one that is far more effective than simply protecting critical infrastructure against natural and man-made threats. Protection is reactive. It cedes the initiative to the enemy.

Limits of Protection. Lack of initiative in developing a protective strategy is particularly problematic as societies become more complex. Advanced societies have far greater vulnerabilities. Despite its land mass, affluence, and population, the United States has many vulnerabilities, even critical ones, from food and water supplies to the Internet. Spending billions to protect infrastructure does not make the nation invulnerable. If the government hardens one group of targets, such as nuclear power plants, terrorists can simply shift to other targets, such as shopping malls.

It is impossible to protect every target, and a strategy predicated on protection is bound to fall short. The enemy will find something else to attack. Since the core of the strategy is to prevent damage to infrastructure, once an enemy achieves such damage in an attack, the perception will be that the strategy abjectly failed.

The U.S. government's pursuit of an unobtainable goal in protecting infrastructure—"failure is not an option"—has resulted in a growing list of "critical" infrastructure. The nation has reached the point where the designation is more and more pointless. If everything is critical, nothing is critical. Politics and stakeholder interests increasingly drive investments in what should and has to be protected rather than rational assessments.[8]

In contrast, resiliency promises something much more achievable and important: sustaining society amid known threats and unexpected disasters. Indeed, the more complex the society and the more robust the nature of its civil society, the more it should adopt a strategy of resilience.

Elements of Resiliency

Strategies combine the ends, ways, and means by which a government uses the instruments of national power to achieve national objectives. What follows are elements of a model strategy of resiliency.

Communicative Action. The fundamental goal of a government's resiliency strategy is communicative action to reassure the society that its way of life can and will be maintained despite threats. Communicative action may be considered in two parts.

The first is the pre-crisis or pre-event stage. Here the government's objective is to inform expectations: to communicate what the public reasonably should expect during disaster and disruptions. A government's ability to manage expectations is vital to sustaining its legitimacy.

The challenge of unrealistic expectations was illustrated graphically in the U.S. government's

6. James Jay Carafano, "Improving the National Response to Catastrophic Disaster," statement before the Committee on Government Reform, U.S. House of Representatives, September 15, 2005, at *http://www.heritage.org/Research/HomelandSecurity/tst091505a.cfm*.
7. James Jay Carafano and Richard Weitz, "Enhancing International Collaboration for Homeland Security and Counterterrorism," Heritage Foundation *Backgrounder* No. 2078, October 18, 2007, at *http://www.heritage.org/Research/HomelandDefense/bg2078.cfm*.
8. "Container Security at U.S. Ports: The Heritage Foundation's Research," Heritage Foundation *WebMemo* No. 1260, November 27, 2006, at *http://www.heritage.org/Research/HomelandSecurity/wm1260.cfm*.

response to Hurricane Katrina, the devastating storm that struck thousands of square miles in three states and disrupted the lives of millions. Contrary to popular perception, the government response—despite miscues at the local, state, and federal levels—proved sufficiently effective to avert a large-scale human tragedy. However, expectations of what government should and could do were out of scale with reality. These unrealistic expectations, fueled by media reports and political posturing, greatly undermined the legitimacy of the national response.

For governments, the lesson of Katrina and similar disasters is that officials cannot do much to inform and moderate expectations after disaster strikes. Officials must establish legitimacy, trust, and confidence before a crisis—with its accompanying raw emotions—erupts.

The second component of communicative action is crisis communication: sustaining the government's legitimacy during and immediately after a disaster. Effective crisis communication must be understandable, credible, and actionable. Those who receive the message must *understand* that it is an emergency message and be able to comprehend and interpret the contents. They must believe that a real threat requires a response from them, and they must be told what action they need to take to guard their safety and security.[9]

The goal, or end, of a resiliency strategy is to instill public trust and confidence in the national response. That stability in turn will allow time for public–private partnerships to address material problems, adapt, and begin to return conditions to normal.

Responding to Risks. The principal method for organizing a strategy of resiliency is to determine how to understand and respond to risks. As Paul Rosenzweig and Alane Kochems noted in a previous Heritage study:

> Risk is uncertainty. It is both the uncertainty that surrounds actual events and outcomes and the uncertainty that surrounds future, potential events. It may, of course, apply to natural events (like the risk from hurricanes) and to non-physical events (like the risk from changes in the financial markets). As relevant to Homeland Security issues, however, risk is more particularly the likelihood that a terrorist threat will endanger or affect some asset. That asset can be an individual (like the President), a structure (like the Pentagon), or even a function (like America's stock exchange system).[10]

Quantifying and determining optimal responses to risk is called risk management. This process includes an assessment of risks and an action plan to reduce risks. In the arena of homeland security, a risk assessment involves evaluations of threat, vulnerability, and criticality:

> *Threat Assessment.* The probability of an attack includes several separate components. It involves, first, an assessment of near-term threats (based, in part, on things like current intelligence and an analysis of the adversary's intentions). In other words, we ask, based upon what we know, what is the likelihood of activity against a particular individual, asset, location, or function.
>
> We then conduct an evaluation of the adversary's capabilities. What can he accomplish with what degree of lethality or effect? Perhaps the biggest change that resulted from September 11 is that we have to fundamentally reassess our adversary's capabilities. When the Soviet Union was the adversary, the capabilities were measured by army divisions and nuclear warheads. Now, they are measured by box cutters. This portion of the assessment is often called the "Threat Assessment."

9. U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, *Communicating in a Crisis: Risk Communication Guidelines for Public Officials*, 2002, pp. 24–25, at *http://www.riskcommunication.samhsa.gov/RiskComm.pdf* (October 25, 2007).
10. Paul Rosenzweig and Alane Kochems, "Risk Assessment and Risk Management: Necessary Tools for Homeland Security," Heritage Foundation *Backgrounder* No. 1889, October 25, 2005, at *http://www.heritage.org/Research/HomelandSecurity/bg1889.cfm#_ftn3*.

Vulnerability Assessment. The probability of success (or failure) looks at the other half of the question: What are our vulnerabilities and how can they be mitigated? It involves identifying weaknesses in structures (sometimes physical; more frequently today, cyber structures), other systems, or processes that could be exploited by a terrorist. It then asks what options there are to reduce the vulnerabilities identified or, if feasible, eliminate them.

Criticality Assessment. The consequences factor is intended to evaluate the effect that will be achieved if the adversary accomplishes his goals. Often the goals will include killing individuals, but they may also include social and economic disruption and psychological effects. Not all consequences can be prevented. So in order to assist in prioritization, there is a process designed to identify the criticality of various assets: What is the asset's function or mission and how significant is it?[11]

Roles in Resiliency. Key to implementing risk assessments in public–private partnerships is establishing the appropriate role of each actor in this joint activity. Understanding, communicating, and reducing threats are primary responsibilities of a national government in ensuring public safety and providing for the common defense. It is not the job of the private sector to defeat terrorists. It is the responsibility of the national government to prevent terrorist acts through intelligence gathering, early warning, and domestic counterterrorist programs.

Determining the criticality of assets, however, should be a shared activity. In many cases, the private sector owns or is responsible for managing both private and public infrastructure that provide vital goods and services for the society. Meanwhile, only the national government has the overall perspective to determine national needs and priorities during disasters and catastrophic threats. The private sector and the national government ought to work together to determine what is truly critical to maintaining the heartbeat of the nation at a time of adversity.

The issue of vulnerability should be the primary responsibility of the partner that owns, manages, and uses the infrastructure, so it is largely the private sector's duty to address vulnerability by taking reasonable precautions in much the same way that society expects the private sector to take reasonable measures for safety and environmental protection. Equipped with these assessments and a common-sense division of roles and responsibilities, public–private partnerships ought to be able to institute practical measures to reduce risk and enhance resiliency.

Governments should participate in defining "reasonable" as a performance-based metric and in improving information sharing to enable the private sector to perform due diligence (i.e., protection, mitigation, and recovery) in an efficient, fair, and effective manner. A model public–private regime would define what is reasonable through clear performance measures, create transparency and the means to measure performance, and provide legal protections to encourage information sharing and initiative.

Marshalling Means

In deciding which elements of national power to apply to a strategy of resiliency—that is, the question of means—governments should approach the use of national security instruments with caution. National security is not about trying to childproof a country against every potential misfortune. It is the task of protecting the country's people from their mortal enemies: other people. These enemies may represent states, trans-states, or no states at all. They may be abroad or homegrown.

What the enemies have in common is that they threaten the nation by preparing to attack its people for a political purpose. Unlike criminals, those who threaten national security are not in it for personal profit. They are out to harm the nation and its people. Properly defined, other dangers—from illegal immigrants to diseases—may be considered national security problems, but they are not national security threats.

National Security and Resiliency. There are good reasons not to dilute the definition of national

11. *Ibid.*

security to include a plethora of threats or to use the proliferation of threats to broadly scope a national resiliency strategy. First, government has resources to address all kinds of problems. Resources, however, are not infinite. Government should reserve national security instruments for the critical task of battling those who are plotting to kill citizens, undermine the society, and destroy individual freedoms.

A second reason not to label every danger *du jour* a national security threat is to protect the civil society. In times of peril, the nation should rely on the government to provide for the common defense, supplying the leadership and resolve to meet imminent dangers. That is why, for example, the President of the United States is vested with the authority to conduct foreign policy and act as commander in chief. The Constitution envisioned an executive who could wield significant power to act decisively in time of war or other crisis.

That said, the President's national security powers should be reserved only for serious, imminent dangers from America's enemies. Elevating such issues as global warming, pandemics, or energy supplies to the level of national security only encourages government to bring the extraordinary powers of the executive branch to bear. This is a terrible idea—one that conceivably could lead a President to dictate energy and environmental policies unilaterally in the name of national security, bypassing market-based solutions, community responses, or other societal means to address the challenges more effectively.

Practical Considerations. At times, government uses national security instruments to do other things, and there are practical reasons for this. The Department of Homeland Security (DHS), for example, responds to transnational terrorist attacks as well as to domestic natural disasters. This is because the nation has one emergency-response system. When a disaster happens, police cars and fire trucks show up regardless of whether the disaster is man-made or heaven-sent.

In times of crisis, the nation cannot have its first responders sitting around and waiting for an official determination of whether an explosion or fire is the result of al-Qaeda or an accident. Likewise, the United States and many other countries often use their militaries to help respond to natural disasters, but that does not make these crises matters of national security.

For the most part, government agencies charged with national security should stick to hunting terrorists, thwarting rogue states, and countering other serious enemies who spend their days and nights plotting against the state. A strategy of resiliency should rely primarily on other instruments of power.

A Legal Framework. Resiliency's role in protecting society transcends homeland security and other national security concerns. Resiliency is about building strong, cohesive societies that can prevail against many challenges, from the heartless whims of Mother Nature to the malicious acts of terrorists.

Indeed, rather than national security instruments, the most common tool that needs to be forged for building resiliency is a legal regime that allows the private sector and marketplace to adapt and innovate, to develop a robust, redundant capacity to provide goods and services—especially in times of crisis.

Liability and Resiliency

Addressing concerns of liability under the law may be the most vital contribution that governments can make to implementing strategies of resiliency. One knotty challenge in promoting public–private cooperation to combat terrorism was highlighted in the recent bitter debate between Congress and the Administration over extending immunity from civil suits to telecommunications companies that cooperated with a classified government surveillance program.[12]

Creating Space for Initiative. Liability protections, such as providing "safe harbors" for sharing critical information and promoting cooperative

12. James Jay Carafano, Robert Alt, and Andrew Grossman, "Congress Must Stop Playing Politics with FISA and National Security," Heritage Foundation *WebMemo* No.1791, January 31, 2008, at *http://www.heritage.org/Research/LegalIssues/wm1791.cfm*.

joint action for public–private partnerships, create the space for the private sector to take the initiative.

For example, the U.S. government acted decisively and with good effect in the case of the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act. Passed in 2002, the SAFETY Act lowered the liability risks borne by providers of products and services for combating terrorism. The law protects the incentive to produce products designated as "qualified antiterrorism technologies" by the Secretary for Homeland Security. The DHS made a concerted effort to implement the program, and companies took the opportunity to obtain certification under the SAFETY Act.

By addressing the issue of liability, Congress intended the SAFETY Act to serve as a critical tool for promoting the creation, proliferation, and use of technologies to fight terrorism.[13] The law provides risk- and litigation-management protections not only for makers of qualified antiterrorism technologies, but also for others in the supply and distribution chain. It created limitations on liability in third-party claims for losses resulting from an act of terrorism in which the technologies were deployed to help prevent or mitigate the danger. In turn, promotion and deployment of the technologies help make society more resilient.

Venues for Collaboration. Other nations should consider establishing liability-protection regimes as well. Collaboration could begin with the Technical Cooperation Program (TTCP), an international organization for sharing defense-related scientific research and technical information. With Australia, Canada, New Zealand, the United Kingdom, and the United States as members, it is one of the world's largest collaborative forums for science and technology.

U.S. partners in Asia, including Japan, Australia, New Zealand, Taiwan, South Korea, India, Hong Kong, and Singapore, also may be sources of international cooperation. Already, Singapore is America's 15th-largest trading partner and ninth-largest export market. Foreign direct investment in Singapore is concentrated in the technical service, manufacturing, information, and professional scientific sectors.[14]

Promoting liability-protection regimes should be the centerpiece of efforts to expand bilateral participation across the globe in developing resiliency strategies.[15]

Forums for Resiliency

Both within its borders and with international partners, the United States should begin to establish regular forums to promote the resiliency concept, share best practices, and pave the way for joint action.

Regional DHS Offices. In the U.S., these forums could encourage a regional structure for homeland security that promotes voluntary cooperation among states, local communities, and the private sector. The Homeland Security Act of 2002 required the DHS to set up a regional structure, but department officials did not follow through on this requirement.

State-based programs would focus on ensuring that the states are prepared to sustain themselves. Successful programs would not emphasize federal structures, but rather would emphasize regional emergency-management programs and capabilities that states develop, coordinate, and run. Similar small-scale programs using a regional model, such as the Emergency Management Assistance Compact (EMAC), already have proven successful.

Local Preparedness. Expanding on the EMAC idea and focus, DHS regional offices should be required to strengthen state and local preparedness. They should improve regional cooperation among governments, the private sector, and non-governmental organizations, and they should plan and

13. U.S. Department of Homeland Security, *Final Rule of the Implementation of the SAFETY Act*, Vol. 71, June 2006, at *http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/06-5223.htm* (March 2008).
14. Office of the U.S. Trade Representative, "Singapore," at *http://www.ustr.gov/World_Regions/Southeast_Asia_Pacific/Singapore/Section_Index.html* (March 7, 2008).
15. For specific recommendations, see James Jay Carafano, Jonah J. Czerwinski, and Richard Weitz, "Homeland Security Technology, Global Partnerships, and Winning the Long War," Heritage Foundation *Backgrounder* No. 1977, October 5, 2006, at *http://www.heritage.org/Research/HomelandSecurity/bg1977.cfm*.

conduct exercises with federal entities that support regional disaster response. These regional DHS offices would enable state and local jurisdictions and their partners to access and integrate capabilities quickly and to improve preparedness and resiliency initiatives.[16]

Global Forums. Internationally, the United States should use existing institutions and new multinational and bilateral partnerships to create forums on resiliency. NATO's Industrial Advisory Group, for example, solicits advice from the defense industry on how to promote public–private and transnational cooperation on defense issues. This group or other NATO forums present opportunities to discuss resiliency issues.

Resiliency's Building Blocks

Talk, however, is not enough. In the end, public–private partnerships must produce the infrastructure necessary to sustain 21st century societies amid 21st century threats. Within the U.S., the national infrastructure is aging and has not kept up with the demands of a growing population. For all of the focus on critical infrastructure, the resiliency of the global economy is equally vital.

Societies must innovate and experiment to speed development of modern infrastructure. One option is to encourage public–private partnerships that invest in public infrastructure. The U.S. has used this model for highways and other projects. Governments and private companies should explore the creation of other opportunities to work together on improving infrastructure.

For example, the U.S. government might consider turning back the Highway Trust Fund and similar federal trust funds to the states or allowing states to opt out of such programs in return for agreeing to make investments that meet quantitative performance measures (such as speeding border-crossing times at ports of entry and exit).

Alternatively, rather than relying heavily on public funding to subsidize maintenance of infrastructure, governments should turn to "project-based" financing to shift risks and rewards to the private sector. States, for instance, would obtain stand-alone investment from a private source or multiple private sources, each with a different level of investment, rate of return, and timeline for realizing returns.

Such strategies not only would shift risk to the private sector, but also should lead to improved decision-making about needed investments in infrastructure.

Conclusion

Resiliency is the right strategy for the United States, its friends, and its allies in facing the dangers of the 21st century. Congress and the Administration should promote this approach within American communities and in all free nations by:

- **Establishing** better public–private models for risk management,
- **Fostering** bilateral cooperation on liability protection,
- **Developing** national and international forums to increase collaboration, and
- **Innovating** to develop resilient public infrastructure for the 21st century.

Governments and their private partners, in adopting these resiliency initiatives, will be able to achieve more than reasonable, cost-effective means to ensure the continuity of services and processes. They also will have become partners in building a civil society that is better prepared to face the future with confidence.

—James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.

16. Jill Rhodes and James Jay Carafano, "State and Regional Responses to Disasters: Solving the 72-Hour Problem," Heritage Foundation *Backgrounder* No. 1962, August 21, 2006, at *http://www.heritage.org/Research/HomelandSecurity/bg1962.cfm*.