Concept Development: An Operational Framework for Resilience

August 27, 2009

Prepared for
Department of Homeland Security
Science and Technology Directorate

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE
2900 South Quincy Street • Suite 800
Arlington, VA 22206-2233

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
27 AUG 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Concept Development: An Operational Framework for Resilience	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Department of Homeland Security,Homeland Security Studies and Analysis Institute,2900 South Quincy Street Suite 800,Arlington,VA,22206-2233	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**52**	

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185) , herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers or FFRDCs to provide independent analysis of homeland security issues. Analytic Services Inc. operates the HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE (HSSAI) as a FFRDC for DHS under contract HSHQDC-09-D-00003.

HSSAI provides the government with the necessary expertise to conduct: cross-cutting mission analysis, strategic studies and assessments, development of models that baseline current capabilities, development of simulations and technical evaluations to evaluate mission trade-offs, creation and evolution of high-level operational and system concepts, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing evaluation in tandem with the government's acquisition process. HSSAI also works with supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise.

HSSAI's research is undertaken by mutual consent with DHS and is organized by Tasks in the annual HSSAI Research Plan. This report presents the results of research and analysis conducted under

Task 09-01.03.02.12 (Concept Development)

of HSSAI's Fiscal Year 2009 Research Plan. The purpose of the task is to develop an integrated and operationally-oriented approach to the concept of resilience in the context of homeland policy and planning.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

HOMELAND SECURITY STUDIES & ANALYSIS INSTITUTE

Jerome Kahan
Task Lead

Andrew Allen
Senior Analyst

Justin George
Associate Analyst

George Thompson,
Deputy Director, Plans and Programs

CONCEPT DEVELOPMENT: AN OPERATIONAL FRAMEWORK FOR RESILIENCE

27 August 2009

Prepared for
Department of Homeland Security
Science and Technology Directorate

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

Analytic Services Incorporated
2900 S. Quincy Street
Arlington, VA 22206
Tel (703) 416-3550 • Fax (703) 416-3530
www.homelandsecurity.org

HSSAI Publication Number: RP09-01.03.02.12-1

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

There is growing interest in the subject of resilience on the part of President Obama's Administration, as well as lively discussion regarding this issue in academic, business, and governmental circles generally. This paper offers an operational framework that can prove useful to the Department of Homeland Security (DHS) and stakeholders at all levels, both public and private, as a basis for incorporating resilience into our infrastructure and society in order to make the nation safer.

Foundations for Resilience

The essence of our approach is to formulate a holistic framework for resilience, accounting for the complexities that provide the basis for operational implementation of practical solutions that incorporate resilience into our critical infrastructure and society. The intent is not to replace current policies, programs, and activities, but to reorient and revise such efforts to reflect the features of resilience.

We see resilience as the aggregate result of accomplishing three objectives regarding critical systems and their key functions. Accomplishment of these three objectives is driven by eight principles. Those principles guide the application of practical ways and means to achieve resilience across the full spectrum of homeland security missions.

The three interrelated, mutually reinforcing objectives or end states that drive our approach are *resistance, absorption, and restoration.*

- *Resistance* is accomplished when the threat or hazard damage potential is limited through interdiction, redirection, avoidance, or neutralization efforts. The actual amount of damage received by targeted critical systems and their key functions, whether physical or societal, is constrained to the extent feasible. The entire system experiences less damage than would otherwise be the case**.**
- *Absorption* is accomplished when consequences of a damage-causing event are mitigated. Effects on quality, equity, and functionality are swiftly contained and reduced to the extent feasible. The system experiences damage, but maintains its structure and key functions. It bends, but does not break.
- *Restoration* is accomplished when the system is rapidly reconstituted and reset to its pre-event status. Damage to critical systems' most vital nodes and pathways have been repaired. Key functions are reestablished, possibly at alternative sites or with substitute processes, and possibly at an enhanced level of functionality.

The eight principles key to achieving resilience are: *robustness, threat and hazard limitation, consequence mitigation, adaptability, risk-informed planning and readiness, risk-informed investment, harmonization of purposes,* and *comprehensiveness of scope.* These principles serve both as conceptual lenses for understanding resilience features and as criteria for realizing resilience objectives. They can help planners designand select ways and means best suited for incorporation into homeland security mission capabilities.

Planning for Resilience

Resilience needs to be planned in advance—*before* systems are damaged and undesired consequences occur. Such planning can be challenging, given the different interpretations currently attached to "resilience," and the complexity inherent in the concept.

Planners need to account for the fact that resilience is both broad and deep. It encompasses both "hard" systems (such as infrastructure and assets) and "soft" systems (such as communities and individuals). It entails economic, societal, and governmental activities. And it impacts stakeholders at all levels. Planners need to bound the planning space—by region, city, or sector—with risk-informed methods that help establish priorities.

Resilience planners can benefit from a method for describing and illustrating the resilience behavior of critical systems and their key functions when these are confronted with specific threats or hazards. A simple but visually direct technique for accomplishing this is to *establish a "resilience profile" for key functions within critical systems.* Such a profile is delimited by three design parameters: *function, latency limit, and minimum performance boundary.* Investment strategies can be developed using these profiles to identify cost-effective ways and means to incorporate resilience capabilities across the homeland security mission spectrum for the system in question. Solutions need to be practiced and tested.

Next Steps

This paper presents a high-level framework for understanding resilience, along with a set of guidelines for operationalizing this concept—translating it into specific policies, procedures, and programs. Operationalizing resilience will require additional analysis and careful attention to detail.

The next steps include answering the following questions:

- What specific areas of further analysis might be given high priority with a view towards making resilience truly operational?
- How might DHS assist the White House staff in making resilience part of our overall homeland security approach?
- How can stakeholder perspectives on resilience at private and public levels be anticipated and accommodated?

Operationalizing the resilience framework presented in the paper will not be easy. But the potential payoff in terms of enhanced economic, individual, and societal security is immense.

1. SETTING THE STAGE

In the aftermath of the September 11th terrorist attacks, and to an even greater extent after the damage wreaked by hurricane Katrina, the concept of resilience has been part of broader efforts to develop policies and programs that seek to secure the homeland against such significant challenges. Attempts to define and apply resilience have occurred against the backdrop of ongoing debates about the brittleness of our aging infrastructure and the readiness of our domestic population to effectively cope with large-scale catastrophes of human or natural origin.

As found in academic and governmental circles, as well as the private sector, there is a wide variety of creative, well-researched, and often countervailing perspectives on the meaning of resilience, its span of coverage, how to implement this concept, and the roles of all homeland security stakeholders. Yet the common theme among these sources is that resilience is important to the safety and security of the nation, deserving recognition as such by decision makers and incorporation with high priority into our homeland security initiatives.

In a report to help in transitioning to a new Administration, the importance of resilience was highlighted by DHS's Homeland Security Advisory Council (HSAC) as one of the top 10 challenges facing the next Secretary of Homeland Security.[1] This emphasis is consistent with the earlier Report of the HSAC Critical Infrastructure Task Force (CITF), which recommended that the Department "promulgate critical infrastructure resilience as the top level strategic objective—the desired outcome—to drive national policy and planning."[2]

In calling for greater national resilience, an influential expert on resilience observed that "the United States is becoming a brittle society … the private sector [should] take the lead in advancing resilience at the company and community levels."[3] The need for resilience in our physical and cyber infrastructure is reflected in the National Infrastructure Protection Plan (NIPP), which for many years has been a major instrument designed to provide "the unifying structure for the integration of existing and future CIKR [critical infrastructure and key resources] protection efforts and resiliency strategies into a single national program."[4]

During the 2008 U.S. presidential campaign, substantial emphasis was placed on the concept of resilience by then-candidate Obama and his spokespersons as a strategic homeland security construct.[5] Until recently, the Obama Administration has been silent on this issue, at least in public.

---

[1] U.S. Department of Homeland Security, Homeland Security Advisory Council, *Top Ten Challenges Facing the Next Secretary of Homeland Security*, Washington, DC, September 11, 2008, pp. 11-12.

[2] U.S. Department of Homeland Security, Homeland Security Advisory Council, *Report of the Critical Infrastructure Task Force*. Washington, DC, January 2006, p. 4; www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf.

[3] Stephen E. Flynn, "America the Resilient," *Foreign Affairs*, March/April 2008, pp. 2-8.

[4] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (NIPP), Washington, DC, 2009; http://www.dhs.gov/files/programs/editorial_0827.shtm.

[5] These positions, calling for resilience to play a central role in safeguarding the nation, were articulated in a number of venues by key Obama advisors. Two examples are "Homeland Security in 2010: Strategy and Resilience in the Face of Global Terrorism: The Candidates' Positions," CSIS, September 9, 2008, and "Resilience in Homeland Security Policy," panel sponsored by the Reform Institute, October 1, 2008.

However, in May 2009, a press report noted that the Administration had established a new National Security Council (NSC) Directorate for Resilience. As reported, this Directorate would focus on "preparedness and response for a domestic WMD attack, pandemic, or natural catastrophe." [6] Although not explicitly tied to the new Resilience Directorate, the White House counter-terrorism (CT) website currently promotes an understanding of resilience that includes the social as well as the physical infrastructure of the nation, with emphasis on working with private and government partners to develop a critical infrastructure protection (CIP) and resilience plan that includes investments in business, technology, civil society, government, and education.[7]

Resilience, in the broadest sense, was also an element in a recent speech by the Secretary of Homeland Security. In presenting a "four-level collective response" to homeland security, the Secretary noted "the urgent need to refocus our counter-terror approach… to make it more layered, networked, and resilient," and referred to resilience as one of the "values that define our nation."[8]

Beyond these characterizations, however, there are few if any public details on what the Obama Administration sees as the mission of the new Resilience Directorate, how it sees the basic issue of resilience as supporting its overall homeland security policy, what practical steps might be taken to implement a policy of resilience, and what role DHS might play in this regard.

Given this situation, the purpose of this paper is to translate the many concepts, constructs, perspectives, and approaches to resilience found in the sources we have reviewed into an integrated and cohesive structure.[9] More specifically, the aim of this effort is to present a practical and policy-relevant framework, including a set of planning guidelines that can be useful not only to DHS but also to stakeholders at all levels, public and private, who share the need and responsibility to incorporate resilience into our overall efforts to better safeguard the nation.[10]

The remaining sections of this paper will

- Summarize challenges inherent in analyzing the complex issue of resilience (section II)
- Present the major building blocks of an operational framework for resilience (section III)
- Provide guidelines for resilience planning (section IV)
- Propose steps for translating resilience from concept to reality (section V)

---

[6] Spencer S. Hsu, "Obama Integrates Security Councils, Adds New Offices: Computers and Pandemic Threats Addressed," *Washington Post*, May 26, 2009, p. 4; http://www.washingtonpost.com/wp-dyn/content/article/2009/05/26/AR2009052603148.html.

[7] See http://www.whitehouse.gov/issues/homeland_security.

[8] Remarks to the Council on Foreign Relations, July 29, 2009, http://www.dhs.gov/ynews/speeches/sp_1248891649195.shtm.

[9] We consulted a cross-section of relevant sources, but could not, within time and resource constraints, conduct a truly exhaustive search and assessment of the vast number of sources on this topic. See the attached bibliography.

[10] This paper primarily employs high-level policy analysis in an attempt to provide an overall framework for resilience. We systematically seek to identify and structure an interrelated group of policy objectives, principles, and planning guidelines in order to present the issue of resilience in a practical, internally consistent, and coherent manner. Further, more detailed policy analysis can be employed to investigate specific resilience issues. Other techniques, such as systems analysis, program analysis, and economic analysis, offer complementary methods for addressing various dimensions of the this complex subject. See, for example, Robert Edson, *Systems Thinking Applied*, Analytic Services, December 3, 2008.

2. CHALLENGES IN ANALYZING RESILIENCE

Even if limited to the realm of homeland security, understanding and analyzing the resilience problem space is difficult and poses many challenges. Definitions, interpretations, and analyses addressing this concept come from all directions—from corporations to citizens, engineers to social workers, government officials to academic researchers—and from abroad as well as home. There are significant differences in stating the exact nature of the questions that need to be addressed.

The concept of resilience in the homeland security context is inherently complex and multidimensional, with many dynamic and interrelated parts. It has a broad range of applicability, from physical assets and industrial infrastructure to citizens and communities. A variety of methods can be employed to discover and solve problems in an attempt to produce useable solutions. Whatever approach is taken, tensions, dilemmas, and trades need to be considered.

Adding to the analytic complexities are the political complexities associated with obtaining input and buy-in from the major public and private stakeholders at all levels, all with their own perspectives and interests. Resource constraints and competing demands will limit the degree to which either public or private funds will be available over the next few years to support practical applications of resilience.

Our proposed operational framework for resilience draws upon the many insightful ideas we found in researching this subject. Given time and resource constraints and the vast array of sources, the research supporting this paper was not exhaustive, but we did review a relevant cross-section of the resilience community, both governmental and academic, as shown in the attached bibliography.

Before presenting our analysis, however, it might be useful to record the nature of the more important challenges inherent in any effort to address this issue: *differing definitions, span of coverage, and understanding interrelationships.*

2.1 Differing Definitions

Many sources present definitions of resilience, which tend to take differing and sometimes inconsistent viewpoints.[11] In researching this paper, we found a number of definitions to be useful starting points:

- Researchers in 2005 offered the following definition, endorsed by the HSAC CITF:

  Resiliency is defined as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.[12]

[11] Referring to the wide range of definitions offered by many experts and in many contexts, often with broad and differing interpretations, one expert argued that "resilience is in danger of becoming a vacuous buzzword from overuse and ambiguity." Adam Rose, "Economic Resilience to Natural and Man-made Disasters: Multidisciplinary Origins and Contextual Dimensions," *Environmental Hazards: Human and Policy Dimensions*, vol. 6 (2007), pp. 1-16.

[12] Brad Allenby and Jonathan Fink. "Toward Inherently Secure and Resilient Societies," *Science*, vol. 309, No. 5737 (August 12, 2005), p. 1034. See the HSAC CITF Report, p. 5, which favors this definition.

- DHS has the following official definition:

  [R]esilience is the ability of systems, infrastructures, government, business, and citizenry to resist, absorb, and recover from or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance.[13]

- With a societal, rather than physical focus, one expert argued the following:

  A resilient community is one that can withstand an extreme event with a tolerable level of losses and takes mitigation actions consistent with achieving that level of protection.[14]

- From a foreign perspective, national resilience is defined as

  The capacity of a society to prepare itself, to contain and effectively manage major national crises, to react in accordance with their severity and magnitude, and to "bounce back" expeditiously to an enhanced functioning.[15]

The range of definitions underscores the challenge of developing a useful framework for turning this concept into practice.

2.2 Span of Resilience

One unavoidable challenge in analyzing resilience is the fact that it spans a wide spectrum of systems, both hard and soft. Hard resilience addresses institutions and infrastructure and refers to their structural, technical, mechanical, and cyber systems' qualities, capabilities, capacities, and functions. Soft resilience, in contrast, refers to the aspect of resilience related to family, community, and society, focusing on human needs, behaviors, psychology, relationships, and endeavors. In either case, organizations of the elements of these broad sets can be usefully thought of as systems with functional components.

Although the hard and soft aspects of resilience have often been addressed separately by different policy and research communities, they are synergistically interrelated. Without institutions and infrastructure, people would be forced to live a very rudimentary, isolated, and precarious existence. Without people, the institutions and infrastructure have no purpose and little ability to endure. Businesses and governments, for example, need to maintain the trust of their employees and their customers (citizens) if they are to remain viable.

It is also notable that these dynamics are seen in areas where populations and infrastructure are frequently subjected to natural disasters. Institutions and communities in these regions grow together in understanding the nature of catastrophic events and recognizing their roles and responsibilities in managing consequences of severe adversity. Confidence is built in their combined abilities to contend with disaster and its aftermath and learn from the event. In the

---

[13] U.S. Department of Homeland Security, *Risk Steering Committee; DHS Risk Lexicon*, Washington, DC, September 2008, pp. 23-24. Other aspects of resilience are also presented.

[14] D. Mileti, *Disasters by Design: A Reassessment of Natural Hazards in the United States* (Washington, DC: Joseph Henry Press, 1999), p. 5.

[15] Meir Elron, "Israel's Homeland Security Concept: From Civil Defense to National Resilience," briefing presented to HSsaI, August 4, 2009.

public and private sectors, the ability of critical systems and key functions to fully recover from a catastrophe depends on the actions of staff, contractors, volunteers, and ordinary individuals.

The synergy that exists between the hard and soft aspects of resilience is illustrated in Figure 1.

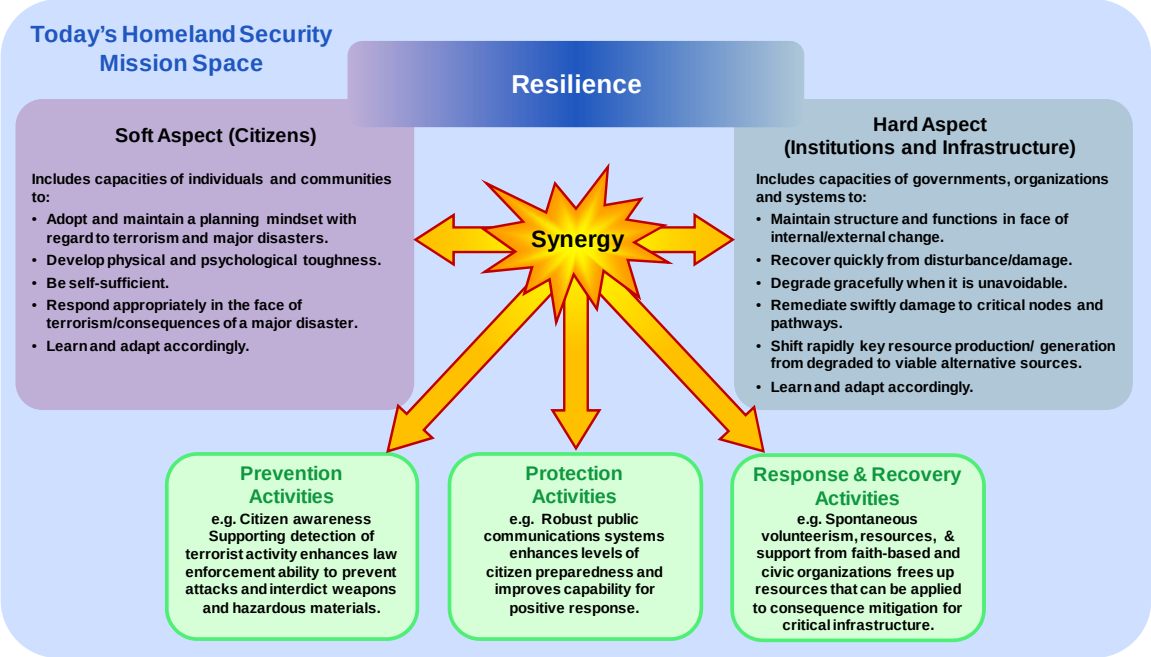


Figure 1: Synergy of Hard and Soft Resilience

In both its hard and soft aspects, resilience applies across three critical areas of American life: society, economy, and government.

> ***In society,*** the concept encompasses societal cohesion and continuity of key social relationships and related activities. Societal resilience emerges through the strength of family relationships and neighborhood ties; the operations of religious institutions, fraternal, and community service organizations; and the connections of clubs and other sorts of groups organized to promote citizenship, positive common interests, and quality of community life. Societal resilience is greatly enhanced when these various groups actively prepare to deal with severe adversity and adopt sound practices to maintain their readiness to effectively cope with the prospect, impact, and consequences of disaster. The more complex the society and the more robust its civil relationships, the more it needs those resources that enable it to be resilient. Cities and communities are often used to capture essential forms of societal systems. While a city can be thought of as a hard collection of buildings, streets, bridges, sewers, water pipes, and electrical power grids, a community is a soft collection of people who have some distinct and meaningful relationship with one another.

In the economy, the private sector in this nation owns and operatives approximately 85% of the nation's critical infrastructure, spanning both hard and soft features.[16] Without support from the business community, resilience objectives cannot be fully achieved. Many businesses are integrating resilience objectives into their operating models because they view these measures as essential to their long-term profitability.[17] Business resilience emerges through business, corporate, and IT leaders deliberately working together across geographical, functional, business, and decision-making boundaries to build an organization that (in the face of a disaster) rebounds, adjusts quickly, and resumes operations.[18] These include continuity planning that recognizes interdependencies and complements governmental efforts because doing so makes good long-term business sense. But effective application of resilience requires participation across the entire business community in order to encompass all highly vulnerable systems and account for their interdependencies.

In government, resilience involves continuity of government (COG) and continuity of operations (COOP) programs to ensure preservation of government and continuing performance of national essential functions. Continuity also requires that state, local, and tribal governments work to ensure that they are able to maintain or rapidly resume effective functioning during and after catastrophes and are able to interact effectively with one another and the federal government.

In any discussion of resilience, particular note must be given to cyberspace as the nervous system of the nation's critical systems and key functions. It has become, in essence, the control system of the country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber-optic cables that allow a very large portion of our physical infrastructures to work. This vast array of hardware is crucially dependent on people with the proper skills and expertise to ensure its continuing operation and to defend it against both human threats and natural hazards. Thus, there are interrelated hard and soft aspects of cyberspace to be considered.

While adding complexity, the need to address the full span of resilience, as discussed above, is nevertheless essential for describing and understanding how resilience works in a practical sense.

2.3 Understanding Interrelationships

There are the complexities associated with the existence of vast numbers of interconnections and interdependencies among and across systems, both hard and soft and combines. A vulnerability of any one system element potentially creates vulnerability for every other system it touches.

---

[16] Jena Baker McNeill, "Backgrounder: Building Infrastructure Resiliency: Private Sector Investment in Homeland Security," Heritage Foundation, Washington, DC, No. 2184, September 23, 2008, p. 4.

[17] HASC CITF Report, p. 5. In this connection, a report addressing the "business case" for resilience concluded that "the ability to manage emerging risks, anticipate the interactions between different types of risk, and bounce back from disruption will be a competitive differentiator for companies and countries alike in the 21st century." Report of the Council on Competiveness, June 2007, cited by Flynn, p. 6.

[18] One oft-cited example of a company's resilience is the manner in which Wal-Mart responded to Hurricane Katrina, standings as a model for what the government and other private organizations might apply. See "Hurricane Recovery in a Box," *Local Knowledge*, No. 1 (summer 2008), pp. 48-55.

Consequently, since vulnerabilities have the potential to propagate across the whole system of the American nation, countervailing capabilities and capacities that address such vulnerabilities for individual systems must, at least in principle, also account for the United States as a whole system. Such attention includes investments that make the overall system better able to absorb the impact of an event without losing the capacity to function.

This challenge is to find ways to isolate, integrate, and analyze all the resilience-related variables in play, as well as their interactions. Both qualitative and quantitative methods can be applied. Alternative solutions and trades might arise and would need to be compared. From a practical standpoint, all methods need to acknowledge that it is not possible to incorporate resilience into all systems at once. Ways need to be found to prioritize such efforts.

3. OPERATIONAL FRAMEWORK FOR RESILIENCE

The essence of our approach is to formulate a holistic framework for resilience, accounting for the complexities that can provide the basis for operational implementation of practical solutions for incorporating resilience into our critical infrastructure and society. The intent is not to replace current policies, programs, and activities, but to reorient and revise such efforts to reflect the features of resilience.

We see resilience as the aggregate result of achieving specific objectives in regard to critical systems and their key functions, following a set of principles that can guide the application of practical ways and means across the full spectrum of homeland security missions.

One way of understanding what is meant by the all-important concept of "critical systems and their key functions" is to recognize that some systems are more central than others to the normal operations of the domain in which they exist, be it hard or soft. In any particular instance, a function of a given system becomes key by performing a more vital role than functions within other systems. Such a function can participate in a much larger number of connections and/or dependencies. Establishing the presence of such key functions endows their host system with a critical quality.[19]

3.1 Objectives of Resilience

The objectives (or end states) of resilience that underpin our approach are *resistance, absorption, and restoration.* As will be shown, the achievement of these resilience objectives is what ensures that the critical systems of American society, economy, and government can effectively continue in their key functions when challenged by major threats, whether advanced deliberately or via acts of nature.[20] Indeed, a basic tenet of our approach to resilience is to maintain the key functions of critical systems, both human and technical, pending restoration.

To achieve the three objectives identified above, a variety of ways and means for preventing, protecting, responding, and recovering can be combined to create capabilities, both active and passive. When effectively applied, such capabilities do the actual work of countering the damage potential of emerging threats and hazards, containing or deflecting the actual damage received by targeted critical systems and their key functions, and then remediating that damage. Below, we generally describe such "countermeasures" in association with each objective.

---

[19] In our discussion, a function is essentially a node or hub within a "scale-free network." Such networks are dominated by a relatively small set of nodes connected to many other sites. The Internet is a prime example. A scale-free network is one in which some hubs appear to have an unlimited number of links and no node is typical of the others. These networks behave in certain predictable ways. They are quite resistant to accidental failures, but they tend to be extremely vulnerable to coordinated attacks. Destruction of hubs quickly breaks apart the network. Scale-free networks can be contrasted with "random" networks, which consist of nodes with randomly placed connections. The U.S. highway system is an example of a random network. See Albert-Laszlo Barabasi and Eric Bonabeau, "Scale-Free networks," *Scientific American*, vol. 288, no. 5 (May 2003), p. 60. For a further discussion of how hubs in scale-free networks enable the propagation of vulnerability, see Fan Xiao Wang and Guanrong Chen, "Complex Networks: Small-World, Scale-Free and Beyond," *IEEE Circuits and Systems Magazine*, first quarter 2003, pp. 15-16.

[20] This view of resilience is aligned and consistent with the perspective put forth in the HSAC CITF Report, which characterizes resilience as a strategic objective – that is, a desired outcome, not as discrete defining actions that many definitions of resilience put forth. See Report, p. 6.

Resistance

In the desired end state for this objective, the threat or hazard damage potential is limited. Damage mechanisms employed by human threats are interdicted and defeated and those associated with natural hazards are redirected, avoided, or neutralized where possible. As a result, the damage potential of the threat or hazard is attenuated, and the actual amount of damage received by the targeted critical system and its key functions is constrained to the extent feasible (including zero damage, if that is achievable). Most definitions of resilience do not address the issue of resistance, which we see as integral to a holistic perspective. Of the several definitions we have found in our research, the only one that specifically links resistance-related activities to resilience is that proposed by DHS in its Risk Lexicon document. In this end state, more than just a single damage mechanism would have been addressed. Resistance addressed the fact that the life cycle of a threatening or hazardous situation can include the approach of multiple potential damage mechanisms (human- or nature-driven) dispersed in space and time. Indeed, prudence suggests that incoming damage mechanisms of human threats or natural hazards should be expected to appear in combination, in sequence, or in other mixtures as fits their intent or character.

Countermeasures against threats and hazards in place and contributing value before and during the actual damage or disturbance event can be broadly categorized as active or passive.

- Active resistance countermeasures against human threats include intelligence, law enforcement, and security personnel that seek to identify and interdict threatening individuals or groups and defeat as many of their weapons as possible before they can be used. Active countermeasures against natural hazards tend to focus on avoidance of the hazard through activities such as evacuation.
- Passive resistance countermeasures against human threats include walls, fences, stand-off distance, and other physical barriers that thwart or redirect the efforts of bad actors. Passive countermeasures against natural hazards tend to be of the same sort: barriers that function to thwart the progress of a natural hazard or redirect its flow. Examples are artificial tidal barriers or natural wetlands that prevent flooding of coastal cities or firebreaks that shift the movement of wildfires away from homes and businesses.

Securing strategic warning and tactical warning is a particularly critical prerequisite for effectively achieving the desired end state of limiting the damage potential of both human threats and natural hazards. While some array of threat or hazard countermeasures should certainly be in place before the initial indications of an adverse situation emerge, the longer the amount of lead time available after warning, the greater the number of countermeasures that can be applied, where possible, to the threat and the sooner such countermeasures can be brought to bear.

To the extent that countermeasures are successful in limiting the damage potential of a threat or hazard, they help to set conditions that will affect achievement of the absorption and restoration objectives. More particularly, these countermeasures make it more cost-effective to meet the absorption and restoration objectives because the damage-limited resistance end state serves to lessen the burdens that will have to be addressed to achieve them.

Absorption

In the desired end state for this objective, consequence effects are mitigated. In general, this means that the effects on quality, equity, and functionality generated by damage that accumulates within the targeted system are swiftly contained and reduced to the extent feasible. Specifically, this means that the targeted system has maintained its structure and key functions in the face of internal and external change and has recovered quickly from damage or disturbance. It is important to remember that critical systems almost always perform more than one function. Some of these will be essential in character, while others will be peripheral. In either case, if system degradation has been unavoidable, then this condition has only manifested itself slowly and gracefully.

Countermeasures that support the absorption objective by mitigating consequences are in place and contributing value before, during, and after the damage event occurs (that is, when damage is received by the targeted system). Value flows from their existence as a ready supply of countervailing support and aid in the event of an unexpected adverse occurrence. As with resistance, these countermeasures can be both active and passive.

- Active absorption countermeasures include such forces as security, damage control, and maintenance personnel that either act prior to a damage mechanism's arrival to implement physical reinforcement, bracing or bolstering procedures ("battening the hatches"), or react following a damage event to restrict and reduce consequence effects before they degrade the key functions of the targeted system below acceptable levels and before effects can spread to damage other connected or dependent systems.
- Passive absorption countermeasures against consequence effects include such features as damage-resistant and damage-tolerant design and construction features of facilities and systems (including IT systems) that serve to contain, soak up, or deflect consequence effects within the targeted system and prevent them from reaching and affecting key functions.

A particular countermeasure or strategy can exhibit both active and passive attributes. For example, redundancy can include both passive components (such as a structural member of a building) and active components (such as a backup computer or machine that can be quickly brought on line when primary system elements are degraded or destroyed).

These consequence countermeasures, to the extent that they are successful in containing and reducing the results of the damage event, help set conditions that will affect achievement of the restoration objective. If consequence effects are minimized, fewer resources need to be expended to achieve the restoration end state.

Restoration

In the desired end state, the targeted system is remediated. This means that degraded key functions of the critical system are, to the extent feasible and warranted, rapidly reconstituted and

reset to their pre-event state in terms of quality, equity, and functionality.[21] Damage to critical systems' most vital nodes and pathways has been rapidly repaired. In some cases, the restoration might lead to lower, but still acceptable, levels of functionality. Furthermore, key functions could be reestablished at alternative sites and with substitute ways and means. In some instances, this might have the effect of improving or making more cost-effective the restored functions. Such an outcome would be consistent with the idea that a resilient system or society should be able "to 'bounce back' expeditiously to an *enhanced functioning*" (italics added).[22] This "bonus result," however, need not be the standard against which successful restoration is measured.

As is the case with absorption, measures that support the restoration end state by reconstituting and resetting a targeted system are typically in place and contributing value before, during, and after the damage event occurs (that is, when damage is received by the targeted system). As with *resistance* and *absorption*, these can be both active and passive.

- Active restoration measures include the full repair of all system elements adversely affected by the damage event, including permanent reconstruction or replacement of any system elements irreversibly weakened or destroyed by damage events' consequence. This also includes review and inspection of all temporary or quick repairs effected during immediate reactions to the damage event.[23]
- Passive restoration measures do not directly act to reconstitute and restore the targeted system. Rather, they facilitate delivery of additional resources to support active restoration measures. This includes, for example, the pre-establishment of support relationships with specific vendors or contractor organizations, whose services will be critical to carrying out required reconstruction or replacement of system elements. It may also include the stockpiling of key materials or pre-identification of personnel with knowledge or skill sets critical to implementing active restoration measures.[24]

As can be seen from the foregoing discussion, the three resilience objectives are interrelated and reinforcing. For example, as suggested earlier, the more effectively the resistance objective is accomplished for a targeted system by attenuating if not eliminating the potential of a damage mechanism, the more cost-effective it will be for the other objectives to be realized. If this

---

[21] "Reconstituted" means that a system has been fixed so that it has all of its intended and necessary parts. "Reset" means that the fixed system has been put back into a condition or a state where it is ready and able to perform its functions. Something can be reconstituted but not reset (it will then likely not function, even with all its parts). Something can also be reset, but not reconstituted (it will function badly or fail because it will be missing parts or have damaged parts).

22 See the definition put forward by Elran earlier in this paper.

[23] The actions of Morgan Stanley Dean Witter during the 9/11 attacks provide a case in point. Witter lost one million feet of square space in the disaster, and yet within an hour after the attack, personnel were already operating out of a backup site with senior management operating out of an additional site. Six employees lost their lives, which is significantly less than the losses other companies faced, thanks to implementation of the evacuation plan that was created in the wake of the 1993 attack on the World Trade Center. Harvard Business School, "Leadership on 9/11: Morgan Stanley's Challenge," *Working Knowledge for Business Leaders*, December 17, 2001; http://hbswk.hbs.edu/archive/2690.html.

[24] The Strategic National Stockpile (SNS) is an example of such a measure. It is controlled by the Centers for Disease Control and Prevention (CDC) and consists of medicine and medical supplies that would be necessary to respond to a public health emergency. Centers for Disease Control and Prevention, *Strategic National Stockpile*, July 16, 2009; http://www.bt.cdc.gov/stockpile.

occurred, the system would experience a less significant challenge than would otherwise be the case, with lesser consequence effects to be dealt with in achieving the *absorption* and *restoration* end states.

3.2 Principles of Resilience

The objectives of resilience, as important as they are, do not by themselves define what is meant by a resilient system, nor do they shape the practical ways and means that might be employed to make a system resilient. We see the eight principles, presented below, serving as both a series of conceptual lenses that capture essential features of resilience and as a set of criteria for planners to consult in designing resilient critical systems. While these are presented individually for the purposes of analytic clarity, they are in fact intimately interconnected.[25]

(1) ***Threat and Hazard Limitation:*** Working towards resilience objectives does not begin at the instant that damage occurs. Because of the potentially catastrophic results of being overwhelmed by high-consequence disasters, there is also a need to attenuate the potential of human threats or natural hazards to inflict damage before the hit is taken. This suggests that efforts should be made to anticipate, detect, identify, interdict, neutralize, avoid, or redirect damage mechanisms before they make contact with a target. Limiting the potential of a damage mechanism prior to the system's taking a hit will in turn limit the power of the blow received and better enable the system to recover. The resilience value of threat and hazard limitation actions is characterized principally by time and not necessarily by geography or spatial location. For example, as long as the potential of the attacker to inflict damage is driven to zero, it does not really matter whether a terrorist is stopped fifty feet or fifty miles from a targeted system. The resilience value of the threat and hazard limitation principle is reflected in actions, which may include strategic dispersal of the various key functions of critical systems. Such a measure limits the overall potential of a damage mechanism, even if it arrives at full force, by making it less likely to strike multiple assets in a single event. Notably, its value is also reflected in the intention to address not only single emergent or apparent damage mechanisms, but all that can be detected and identified with regard to a specific threatening or hazardous situation.

(2) ***Robustness:*** This principle indicates the capability and capacity of critical systems to withstand severe internal and/or external stresses and to maintain key functions impacting American society, economy, and government. Robustness includes the capacity to degrade gracefully when this course of action is unavoidable. Categories describing the broad range of scale for such systems include the nation as a whole, regions, cities, programs, industry sectors, specific pieces of infrastructure, buildings, complex facilities and utilities, communities, families, and individuals. Such critical systems must be able to withstand stresses that manifest themselves individually, in combination, or in sequence in order to maintain key functions. Notably, this endurance quality also encompasses the enhanced physical and psychological capacity of individuals and communities to be

[25] For further discussion of a number of the features we describe in the following paragraphs, see T. D. O'Rourke, "Critical Infrastructure, Interdependencies, and Resilience," *The Bridge*, spring 2007, pp. 27-29.

strong, self-sufficient, and capable of appropriate response in the face of the consequences of a major disaster.

(3) ***Consequence Mitigation:*** This principle is founded on recognition of the reality that we cannot always avoid catastrophes. As a result, we need capabilities that enable us to survive the impacts of human- or nature-driven assaults and to manage the consequences of those events. Consequence mitigation incorporates the capabilities and capacities of critical systems and their key functions to control and reduce cascading adverse effects of a damage event and then recover quickly and resume normal activity. The purpose of resilient entities' employing these capabilities is to ensure that they are not overwhelmed and/or immobilized by the results of one or more calamitous events. An important part of this characteristic is the strength that critical systems can potentially draw upon in terms of additional resources (such as funds, materiel, and personnel) through their interconnections and interdependencies with other systems, provided that such support relationships have been established and maintained effective advance planning and readiness efforts.

(4) ***Adaptability:*** This is the principle that enables a resilient system to maintain equilibrium when anticipating a damage event or to return to an equilibrium state after experiencing unanticipated adversity. A resilient system is one that fluctuates because it responds and adjusts to internal and external change. In this regard, resilience is qualitatively different from stability and sustainability, which are merely aspects of equilibrium. A resilient system recognizes that change is inevitable and that it therefore must be able to encounter and adjust to the unexpected without its essential health being threatened. In contrast, stability conveys the idea of a steady-state system with minimal fluctuation. Similarly, sustainability is a static process. Sustainability addresses use of resources to ensure long-term survival and a non-decreasing quality of life. Once resource optimization is achieved, sustainability means continuing at that level.[26]

(5) ***Risk-Informed Planning:*** To ensure that resilience principles contribute to desired resilience outcomes, they need to be implemented in relation to the threat, vulnerability, and consequence (TVC) factors identified for critical systems and their key functions within American society, economy, and government through a thoughtful risk assessment. Successful implementation of the elements of resilience also requires deliberate foresight, intentional prearrangements, and the purposeful development and exercise of required capabilities and capacities to effectively cope with each stage of the life cycle of an adverse situation.

(6) ***Risk-Informed Investments:*** The allocation of resources to investments in meeting the resilience requirements of any critical system or key function needs to be done in a manner informed by an understanding of risks facing those assets. Risk assessments for critical systems (human and technical) and their key functions will all produce descriptions of risk that necessarily differ to a greater or lesser degree.[27] This is so

[26] Rose, p. 386. See also Jamais Cascio, "The Next Big Thing: Resilience," *Foreign Policy*, May/June 2009.

[27] For purposes of this discussion, risk is taken to mean a quantitative or qualitative statement for the set of TVC parameters associated with a particular system (simple or complex) over a given planning period. This is consistent with the definition of risk provided in the *DHS Risk Lexicon*, p. 24.

because the scope, scale, and quality of the three risk elements (TVC) relevant to each system will differ from one case to case another, depending on the level of national life and the mixture of human and technical system features involved. However, if done properly, all such assessments will, in principle, reveal some mixture of requirements for robustness, threat and hazard reduction, and consequence mitigation—including some statement of the associated degree of underlying adaptability required for each.

(7) ***Harmonization of Purposes:*** To be fully effective in serving their purpose, the six principles discussed above need to be mutually reinforcing. How these principles combine can be illustrated as follows: Risk-informed plans for responding to an event to maintain resilience would be developed, and risk-informed investments made, to ensure that the necessary resilience ways and means are established for a given system. Ready assets in place before disaster occurs can help to limit the damage that a threat or hazard is able to generate. This, in turn, will enable an appropriately designed and resourced system to behave robustly and continue critical functions after the conclusion of an expected (or unexpected) damage event. By extension, this will help the affected system to mitigate consequences and return to a *status quo ante* condition. All plans need to stay flexible and adaptive after damage event(s) and work with the specific situation.

(8) ***Comprehensiveness of Scope:*** Finally, standing as a central principle that needs to be taken into account in understanding resilience and developing practical ways and means to make this happen is the recognition that resilience encompasses all of America's national homeland security enterprise, including federal, state, local, and tribal governments as well the private sector, communities, families, and individual citizens, synergistically. Resilience also naturally accounts for the broad span of the homeland security missions, encompassing societal, economic, and governmental areas. Crossing all these areas, as noted earlier, are the hard (physical assets, infrastructure) and soft (communities, citizenry) aspects of resilience, with cyber resilience spanning the entire space.

3.3 Resilience and Homeland Security Missions

One of the major themes found in our review of current governmental and academic sources is the question of whether and how resilience relates to preventing, protecting against, responding to, and recovering from threats to the homeland, whether caused by terrorists or natural disasters, while recognizing that it is not possible to prevent natural disasters in the same way it might be possible to prevent terrorist attacks.[28] These homeland security missions offer a useful structure to develop countermeasures to various threats in the form of on-the-ground capabilities that can lower the likelihood of a damage mechanism reaching a target and to mitigate consequences if

[28] Adverse natural phenomena (hurricanes, floods, earthquakes, lightning-ignited wildfires, and tornados) are clearly not directed or carried out by sentient and malicious agents. In this sense, nothing can be done about natural hazards in terms of thwarting planning, logistics, surveillance, or weapons delivery activities.

such an event were to occur.[29] In other words, effective implementation of these missions can reduce risks for a given situation or class of situations.

There are many views on the relationship of resilience to these homeland security missions, which we summarize below. Often the different views on this issue are associated with particular stakeholders at different levels, both public and private. The more relevant perspectives on this question are discussed below, with comments on how we see these relationships in our operational framework.

Protection

With the NIPP as its main vehicle, the federal government has sought to reach out and engage state and local governments on the need for protection. A great deal of attention has been paid to establishing requirements for critical infrastructure protection across the commonly defined sectors of U.S. industry. Outreach to private-sector stakeholders has been particularly important, since, as noted, they own and operate approximately 85% of the nation's infrastructure. Resilience is an element of these initiatives, but not their centerpiece. Additionally, much of the focus of these efforts is on physical and cyber assets, not on society, community, or citizenry as such.[30]

More generally, it is important to recognize that excessive emphasis on the objective of critical infrastructure protection is not, in itself, an adequate basis for achieving resilience. Indeed, this assessment had led to the observation that "protection, in isolation, is a brittle strategy," inconsistent with the bend-but-do-not-break tenet of resilience.

- Any approach predicated primarily on protection will inevitably fall short when a human adversary finds something else to attack or when a natural hazard manifests itself in an unexpected place. It is impossible to protect every potential U.S. target, and even the most well-protected system can be overcome or penetrated, and, in this case, major consequences can occur.
- Setting the goal of protecting infrastructure at 100%, or what can be called a level of zero tolerance for failure, has resulted in a rapidly growing list of "critical infrastructures." Such expansive application of the "critical infrastructure" designation has badly diluted the meaning of the term in the sense that its usefulness for prioritization has been significantly undermined. In short, "if everything is critical, then nothing is critical."[31]
- Conceiving resilience as being synonymous with protection creates difficulties by leading to the commitment of excessive levels of resources to efforts to protect assets against the most powerful threats or hazards that can be imagined, regardless of their relative improbability. Such an approach will not only risk failing to provide perfect protection to

---

[29] These missions form the centerpiece of 2006 *National Strategy for Homeland Security* and offer an ensuring construct for policy and planning in this field. The White House, Homeland Security Council, *National Strategy for Homeland Security*. Washington DC, October 2007; http://www.dhs.gov/xabout/history/gc_1193938363680.shtm.

[30] The NIPP supports prioritization of protection *and resiliency* initiatives and investments across [CIKR] sectors." NIPP, p. 1 (emphasis added).

[31] Carafano, p. 4. The issue of resilience vice protection is also discussed in the HSAC CITF Report, pp. 5-6.

the chosen systems, but will leave few or no resources that can be applied to support other homeland security missions.

One potentially useful suggestion in the context of resilience vice protection is that the homeland security planning community should begin to think in terms of critical infrastructure *resilience* (CIR), rather than critical infrastructure *protection* (CIP), not as a replacement for CIP, but rather as "an integrating objective designed to foster systems-level investment strategies."[32]

Respond, Recover, Prevent

As suggested, protection does not by itself achieve the objectives of resilience. This requires attention to the connection between resilience and the response and recover missions, as well as the linkage between resilience and the prevent mission.

Resilience has strong associations with response, with this connection most commonly tied to the state, local, and private-sector levels. As the National Response Framework (NRF) recognizes, all disasters, whether driven by activities of humans or nature, are local. Effective response is seen by the NRF as crucial to the resilience of the private sector and is a particular responsibility of prepared individuals working in partnership with local government and nongovernmental organizations.[33]

Resilience typically receives the least attention across all levels of governance when associated with recovery, which seems unusual given that resiliency suggests a need to be able to recover to full functionality after absorbing an attack or hazard. In part, this can be reasonably attributed to the heavy emphasis placed on prevention and response in connection with counter-terrorism in the wake of the 9/11 attacks.[34] However, there are inherent characteristics of recovery that tend to narrow the government's role in carrying out its various activities. Recovery is largely a financial process focused on gathering resources required for rebuilding, tends to demand more than governmental bureaucracies can provide, and is carried out by actors that tend to look to government for only a very limited set of inputs: money, information, and technical assistance.[35]

Lastly, prevention receives a great deal of federal attention, with increasing emphasis on state and local actors, particularly with regard to estimating and seeking to thwart high-consequence threats. But this mission does not appear to be commonly or significantly associated with resilience.

Before moving ahead to discuss the ways and means of resilience, it might be helpful to comment on a question that often arises in homeland security discussions—notably, whether policies and

---

[32] HSAC CITF Report, p. 5. For further discussion of CIR, see George Mason University School of Law, "Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience," CIP Program Discussion Paper Series, February 2007.

[33] U.S. Department of Homeland Security, Federal Emergency Management Agency, *National Response Framework*, Washington DC, January 2008, p. 5.

[34] See Thomas A. Birkland, "Disasters, Catastrophes, and Policy Failure in the Homeland Security Era," *Review of Policy Research*, vol. 26, no. 4 (2009), pp. 226-227.

[35] Robert Olshansky and Laurie Johnson, "Improving Post-Disaster Recovery: Initial Thoughts for a New Administration," University of Illinois, Urbana-Champaign, and Laurie Johnson Consulting; San Francisco, CA, November 17, 2008, p. 1.

programs seeking to safeguard our security, usually centering on the prevent and protect missions, can deter terrorists from initiating attacks.

Without attempting to directly address the elusive issue of deterrence, it is possible to argue that an operationalized approach to resilience, if applied in a practical manner at various levels and for different systems, can present a compelling message to potential adversaries, indicating that any attempted assault will fail to achieve its aims.[36] The dissuasive potential of resilience can be supported by noting that a vigilant and aggressive posture of resilience can increase the level of resources and energy that adversaries must expend to prepare an attack, while raising the cost and uncertainty surrounding their prospects for success. Indeed, not all terrorist attacks can be prevented by incorporating resilience into our most critical systems and their key functions, but adversaries would know that even successful strikes would not cripple our economy or society.

3.4 Resilience Ways and Means

Taking practical steps towards meeting the objectives of resilience is best done by applying resilience-related ways and means to implementing prevent, protect, response, and recover missions, whether addressing physical and cyber assets or the social, business, and community infrastructure. This approach is designed to reinforce, reinterpret, and reorient traditional solutions through the incorporation of resilience-oriented policies, programs, and activities across the full mission spectrum.

While the relationships between the three resistance objectives and the four missions are not simple, the resistance end state is generally serviced by prevent and protect capabilities. The absorption end state is also serviced by protection capabilities, and it receives support from response capabilities. The restoration end state is likewise serviced by the response mission, but it is further serviced by recover capabilities.

Ways and means aimed at meeting the three interrelated resilience objectives need to be applied in an integrated and mutually reinforcing manner across the full mission spectrum, guided by the principles of resilience. For optimum impact, incorporating resilience ways and means into a system when it is in an early design or developmental stage can lead to the most cost-effective results. However, resilience solutions would need to be retrofitted, to the extent feasible, into critical points of our existing national infrastructure, soft as well as hard.

Resilience-related ways and means encompass a variety of capabilities, provided via policies, programs, and activities. They may be material, such as personnel, structures, barriers, networks, hardware, tools, sensors, and supplies of consumable resources like energy, food, and water. They may also be nonmaterial, such as architectures, standards, organizational designs, procedures, methods, techniques, operations, tactics, and training. These capabilities, as noted, are best introduced when systems are under development, but they can be retrofitted into existing systems, both hard and soft. While not exhaustive, the following observations are offered to illustrate the range of options available for identifying and implementing resilience-related ways and means into our critical physical and societal systems:

[36] One expert observed that "decentralizing and reducing the brittleness of necessary global and national critical systems and their key functions demonstrates to terrorists the futility of attacking those systems." Carafano, p. 1.

- Maintaining a diversity of options among inputs and operations associated with key business functions can help us to attain economic resilience. Enterprises that have viable alternatives at their disposal for generating the quantity and quality of outputs needed to sustain business activity and profitability also tend to position themselves to be far more able to sustain serious shocks than those with more limited choices. Examples are developing alternatives for needed parts and training employees in multiple skill sets as well as developing alternative methods for performing key functions.
- Strategic dispersal of the various key functions of critical systems is another sound method for bolstering economic resilience. The virtue in this practice lies in its ability to make it less likely that any damage mechanism that arrives at full potential will be able to strike multiple assets in a single damage event.
- A variety of resilience ways and means can be found in the field of supply chain integrity and continuity of operations.[37] Some of the key characteristics of resilient supply chains are redundancies and alternatives built into all aspects of the life cycle of products and functions (processes, inventories, storage, suppliers, transportation, distributors).
- Included in measures related to enhancing protection, the NIPP mentions "building resiliency and redundancy [and] incorporating hazard resistance into facility design." Other ways and means noted in the NIPP, which can be oriented towards resilience, include "leveraging 'self-healing' technologies, promoting workforce surety programs, implementing cyber security measures, training and exercises, business continuity planning, and restoration and recovery actions."[38]

3.5 Relationships among Elements of Resilience

Figure 2 (below) shows how resilience-related ways and means, filtered through the lenses of the resilience principles, can be incorporated via the homeland security missions to support achievement of the three resilience objectives.

[37] See Yossi Sheffi, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage* (Cambridge, MA: MIT Press, 2005).

[38] NIPP, p. 1.

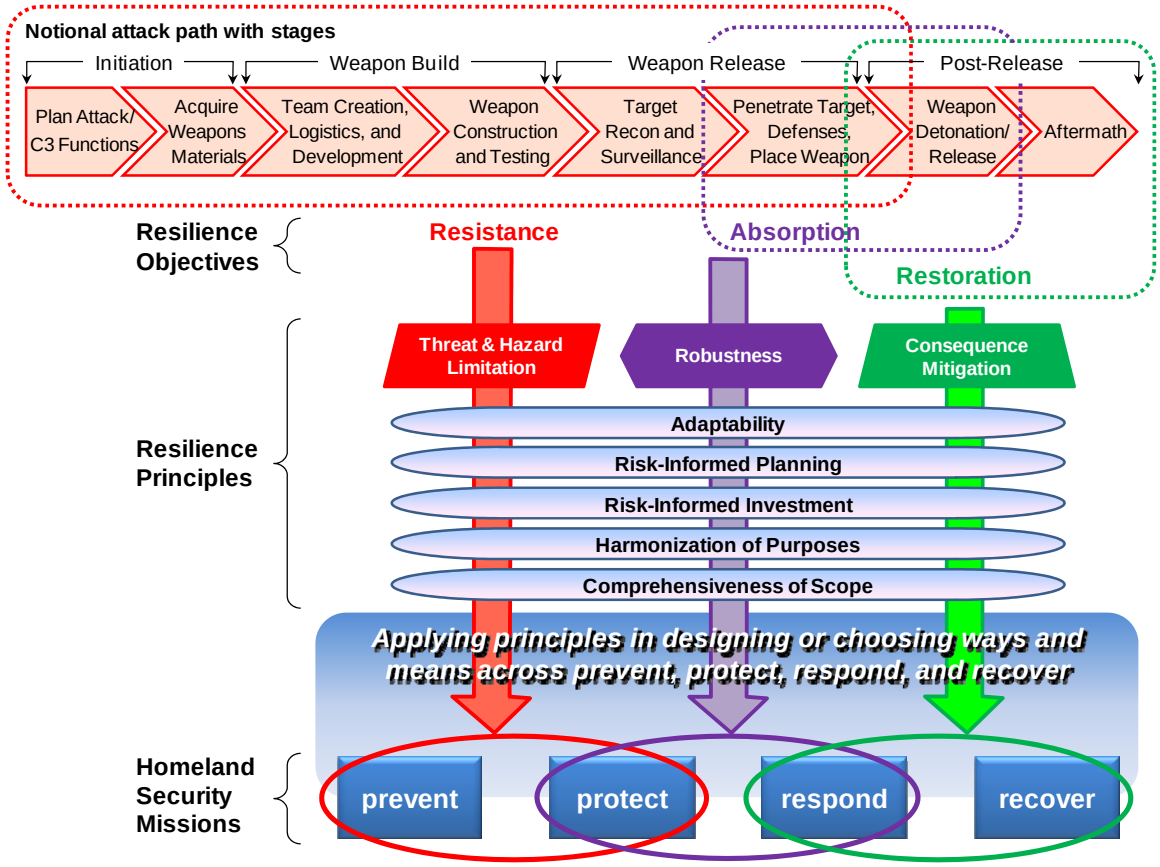


Figure 2: Relations among Elements of Resilience

Consistent with the above discussion, highlights of the major features of Figure 2 can be summarized as follows. For illustrative purposes, the figure shows the elements of resilience under the assumption of a terrorist attack, but its basic construct also applies to natural hazards.

Adversary Attack Path: This provides a graphical depiction of essential steps and stages included in a generic terrorist attack scenario. While simplified to depict a single event, this should not be construed to mean that the life cycle of any particular adverse event will contain only a single damage event. Indeed, adversaries might well apply damage mechanisms in combination, in sequence, or in other mixtures as suits their purpose.

Objectives: Resistance, absorption, and restoration objectives are the combined end-states or outcomes which represent attainment of resilience. While seemingly sequential, these objectives are mutually reinforcing, which reflects itself how the array of resilience elements aimed at meeting these objectives need to be interpreted and applied.

Principles: These serve as conceptual lenses for understanding features of resilience. They also serve as planning criteria to help design or choose practical ways and means from across the homeland security missions suitable for application in achieving resilience objectives.

Ways and Means: These encompass a wide variety of policies, programs, and activities that produce resilience-related capabilities. Ways and means can be judged suitable for resilience-oriented initiatives when they are consistent with the key criteria provided by the principles.

Homeland Security Missions: These prevent, protect, respond, and recover missions provide a practical framework for the incorporation of resilience-related ways and means. Development and execution of policy and program solutions for enhancing resilience need to be accomplished in an integrated manner across the mission spectrum.

3.6 Resilience Illustrated

When the above principles are applied to the design, building, enhancing, and operating of critical systems and their key functions with the aim of achieving the resilience objectives, one should expect to see dramatic differences in how such systems perform in the face of a challenge.

To analytically visualize the effects that application of resilience principles makes in achieving the three desired end states, some method is needed for describing and illustrating the behavior of critical systems and their key functions when these are confronted with specific threats or hazards. A simple but direct way of accomplishing this is to *establish a "resilience profile" for key functions within critical systems*. In the following discussion, we will describe the dimensions and parameters of such profiles and then provide examples of how they can be applied to create an illustrative analytic profile for a key function within a critical system.

Three essential dimensions, *performance, time,* and *gravity,* offer a framework for each profile by providing descriptions of the specific system that needs to be able to meet resilience objectives appropriate for its particular features and environment.

Performance: This dimension describes the general level of capacity and quality at which an element or elements of a system perform an essential role. In regard to resilience planning, it can be conceived of as an aggregate measure of the effectiveness of the key inputs, central operations, and principal outputs of a particular task of a particular system. This idea recognizes that systems frequently perform more than one role. Performance can be measured on a scale running from zero to 100 percent.

Time: This dimension refers to the chronology of the whole life cycle of any particular adverse situation, whether caused by human- or nature-driven hazards. Many but not all life cycles begin with either strategic warning that indicates the emergence of a serious security situation far in advance of an actual damage event or tactical warning that provides a relatively far shorter period before a damage event occurs. Whatever the extent of warning, the resilience time dimension accounts for the possibility that adverse situations may arrive in a single instance, in combination, or in a definite sequence, as mentioned previously. The damage-inflecting dimension of the event concludes when the last damage mechanism makes contact with the target and delivers its effects. But the resilience time dimension continues through the period in which a targeted system reacts to contain and reduce consequence effects and reconstitute and reset itself to its pre-event state, as feasible.

Gravity: This dimension is the quality that determines the degree to which any particular function plays a key role within its host system. Gravity represents the extent to which a particular function within a system of interest performs one or more vital roles in our society, economy, or government and is linked through interconnections and dependencies to other systems in the same or other areas of national life. The more vital the roles that the function and its host system perform and the greater number of interconnections and dependencies in which it participates, the greater its gravity. The importance of a function's level of gravity is reflected in the relative stringency of its allowable resilience performance limits. High-gravity functions will have a relatively small degree of allowable performance degradation under stress. Likewise, they will have a relatively shorter allowable period before they are expected to begin to recover from stress-imposed degradation.

Within a given framework, the resilience profile is more sharply defined by three specific parameters: *function, latency limit,* and *minimum performance boundary*.

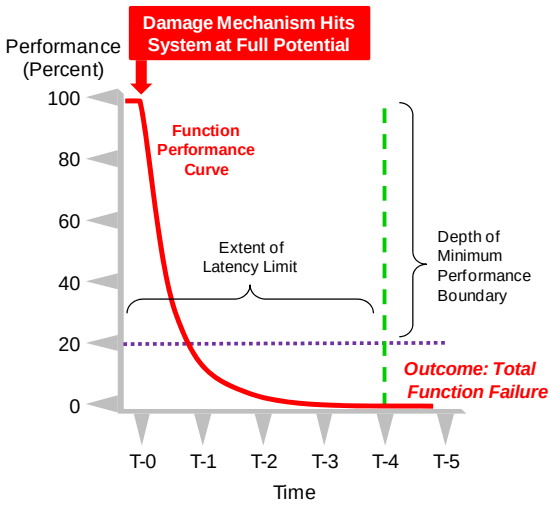
Function: In technical terms, a function is defined as a sequence or architecture of elements that plays one or more roles or performs one or more tasks within a particular system. The most commonly specified elements of a function are its key inputs, central operations, and principal outputs. In practical terms this can relate to things as diverse as an automobile factory's production of cars, the federal government's provision of Social Security benefits to U.S. citizens, or an American family's ability to earn sufficient income to maintain a middle-class standard of living.

Latency Limit: This term describes the maximum amount of time allowable for a function to remain in a degraded or suboptimal state before it must begin to recover. For an automobile factory, this might be days or weeks. For provision of Social Security benefits, this might be weeks to months. For an American family's standard of living, this could be months to years.

Minimum Performance Boundary: This is the lowest acceptable level of performance for the defined function. For an automobile factory, this might be quantified in terms of number of units produced within a set period to achieve a level of profitability that can cover production costs and sustain the business. For the federal government, this might be some minimum percentage of Social Security benefits that citizens have earned in order to keep them above the poverty line. For an American family, this might be a level of income sufficient to provide for basic necessities of food, clothing, shelter, and household utilities.

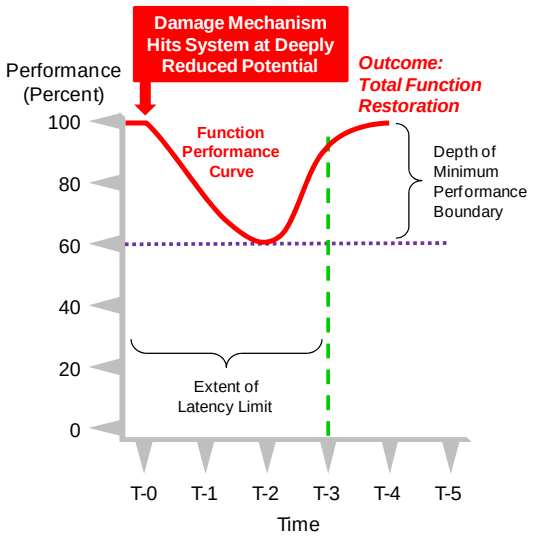
Figure 3 (below) illustrates how the above-referenced dimensions and parameters are combined in a simple and generic fashion to create a visual profile of a function's resilience performance.

Example 1. Key Function in a Non-resilient System



- **Function defined as a company's employee benefit activity.**
- **Function with lower degree of gravity.**
- **Function performance curve shows extreme brittleness.**
- **Damage event occurs at T-0; power of damage mechanism unaffected by system.**
- **Brittle system quickly succumbs to event.**
- **Function performance falls rapidly towards 0% at T-2.**
- **Function performance never recovers.**
- **Event outcome is total function failure at T-4.**

Example 2. Key Function in a Resilient System



- **Function defined as a company's payroll activity.**
- **Function with higher degree of gravity.**
- **Function performance curve shows idealized resilience.**
- **Damage event occurs at T-0; power of damage mechanism reduced by system's resilience features.**
- **Resilient system degrades slowly in response to event.**
- **Function performance stays only briefly at minimum.**
- **Function performance recovers rapidly at T-3.**
- **Event outcome is total function restoration at T-4.**

Figure 3: Expected Function Performance in Non-resilient and Resilient Systems

The *first example* looks at the employee benefit activity (key function) in a non-resilient company, which incorporates few or none of the principles of resilience. The function is relatively low in gravity since most of the employees are attracted to the firm by relatively high salaries and do not depend solely on employer-provided benefits. The company is a brittle system. It has little in the way of effective means of attenuating the potential of a damage mechanism that presents itself. Close to the full potential of a damage mechanism (a category 5 hurricane) is realized when it makes contact with the targeted system (the storm strikes the company's main production center).

- Lacking means planned and implemented in advance to enable it to withstand such a natural disaster and manage its effects, the company quickly loses a large portion of its profitability.
- With no effective means of rapidly reconstituting and resetting itself in the aftermath of the damage event, the employee benefits activity is eliminated as a cost-cutting measure. As employees are not willing to accept a complete absence of benefits, they begin leaving to look for other employers, and the company begins to fail, with little if any prospects for restoration.

The *second example* looks at the payroll activity in a resilient company, which incorporates the full set of resilience principles. It is a situationally aware, tough, and adaptable firm. At a very early point in the approach of a damage mechanism (the category 5 hurricane), it detects and recognizes the emerging adverse situation and brings to bear effective means of attenuating its potential for harm (the company's production facilities were hardened against storm damage and flooding in advance of the hurricane's arrival). Only a small portion of the original potential of the damage mechanism is realized when it makes contact with the targeted system (the production facilities, while somewhat degraded, remain in operation).

- With appropriate means planned and implemented in advance to enable it to withstand such an assault and manage its effects, the function of the system degrades only modestly and for a brief period (company profitability is only moderately affected resulting in small temporary reductions in salary and the three-month deferral of yearly bonuses).
- Possessing effective means of reconstituting and resetting itself in the aftermath of the damage event, the function and its host system recover rapidly to a normal state (salaries and bonuses return to normal one fiscal quarter after the date of the hurricane).

3.7 Summary of Approach to Resilience

The supporting connections among three of the central elements of resilience concept discussed above are are summarized in Table 1.[39]

[39] Please note that in this particular envisioning of the basic relationships among resilience objective, mission areas, and principles the ways and means previously referenced in relation to Figure 1 are merged into the mission areas referenced at the bottom of the table.

Table 1: Crosswalk of Resilience Objectives with Principles and Missions

Resilience Principles	Resilience Objective Supported		
	1. Resistance	2. Absorption	3. Restoration
Threat and Hazard Limitation	✓		
Robustness		✓	
Consequence Mitigation			✓
Adaptability	✓	✓	✓
Risk-Informed Planning	✓	✓	✓
Risk-Informed Investment	✓	✓	✓
Harmonization of Purposes	✓	✓	✓
Comprehensiveness of Scope	✓	✓	✓
Homeland Security Missions Addressed	prevent and protect	protect and respond	respond and recover

From the relationships described in Table 1, the following points are particularly notable:

- Threat and hazard limitation is principally associated with the resistance objective.
- Robustness is principally associated with the absorption objective.
- Consequence mitigation is principally associated with the restoration objective.
- Adaptability, risk-informed planning, risk-informed investment, harmonization of purposes, and comprehensiveness of scope are critical considerations for all three resilience objectives.
- The resistance objective is inherently linked to prevent and protect missions.
- The absorption objective is inherently linked to protect and respond missions.
- The restoration objective is inherently linked to respond and recover missions.

Although not appearing explicitly in either Figure 3 or Table 1, resilience cannot be addressed without recognizing its comprehensiveness of scope. Our approach to resilience is highly sensitive to this issue, which was highlighted in the final principle of resilience presented earlier in this section. As noted, this span of coverage encompasses both the hard and soft aspects of resilience and their interrelations.

In sum, the operational framework presented is based on the recognition that resilience is, in essence, the aggregate result of achieving the resistance, absorption, and restoration objectives over the entire life cycle of an adverse event. These end states are achieved for key functions of critical systems through ways and means usually associated with the homeland security missions that have been reinterpreted, reoriented, and refocused to be consistent with the criteria reflected

in the set of eight resilience principles. Effective implementation of measures to attain resilience objectives, with the inherent flexibility that needs to be part of such solutions, can enhance the capabilities of our society, economy, and government to continually adjust to changing circumstances in the face of human- or nature-driven adverse occurrences. To be effective, a framework for resilience needs to show how policies can be translated into practice through a planning process. This is discussed in the following section.

4. PLANNING FOR RESILIENCE

Planning for resilience needs to be done far in advance of the emergence of any adverse situation that includes one or more damage events. Only through effective planning can the concept of resilience be translated into practical steps to achieve operational resilience.[40]

4.1 Guidelines for Resilience Planning

Resilience planners will face many challenges, as the difficulties of homeland security operational planning in general are compounded by the inherent complexities of resilience.[41] Following are some broad guidelines for assisting planners in meeting these challenges.

> ***Work with Complexity:*** Resilience planning is a necessarily complex effort. This complexity arises out of the large number of stakeholders in the U.S. homeland security enterprise and the vast number of interdependencies and interconnections that exist among critical systems and their key functions across the societal, economic, and governmental areas of American national life. It also arises out of the vast number of possible threats and hazards we may have to confront, both today and in the future. These inherent complexities of the homeland security strategic environment make it necessary for resilience planners at all levels to begin to think more broadly, accounting for resilience requirements that cut across the prevent, protect, respond, and recover homeland security missions. Resilience planning succeeds by acknowledging the complicated nature of the homeland security strategic landscape and finding feasible and tailored approaches for deliberately managing it.
>
> ***Account for Interdependency:*** Achieving resilience objectives depends upon planning and preparedness methods that involve the capacity of planners to effectively appreciate the key risk factors in their operating environments. But planners also need to take an expansive look beyond the narrow situation specific to their own systems (such as network, facility, organization, community, or family) to identify and assess requirements that arise from their broader strategic context. Plans created through processes that are largely isolated and overly restricted in scope ("stovepipes") are likely to fail in execution because they will tend to be surprised when confronted by the adverse effects of ignored vulnerabilities that reach out from other quarters. In some instances, even relatively small points of connection can enable one system's vulnerabilities potentially to spread to affect many others.
>
> ***Establish Priorities:*** Resilience planners need to cultivate a sophisticated understanding of their systems' strengths, vulnerabilities, roles, responsibilities, and relationships. This means developing priorities to ensure that resilience solutions are as efficient and

[40] It might be noted that preparedness in connection with homeland security has many interpretations. We interpret preparedness as encompassing all plans and actions that enable the spectrum of homeland security missions to be executed as a means to lower risk. In this paper we emphasize planning and do not address other elements of preparedness for achieving resilience.

[41] For an insightful assessment of challenges facing crisis planning, see Allan McConnell and Lynn Drennan, "Mission Impossible? Planning and Preparing for Crisis," *Journal of Contingencies and Crisis Management*, vol. 14, no. 2 (June 2006), p. 61.

effective as feasible, given unavoidable limits on resources. Risk-informed guidelines can be used to prioritize evolving implementation efforts by parsing application of resilience measures in terms of threats, vulnerabilities, and consequences relevant to systems, sectors, regions, and communities. For interrelated systems, a planner needs to recognize that not every connection or dependency will carry meaningful exposure to others' vulnerabilities. Indeed, some linkages provide essential conduits through which additional resources and assistance may be accessed during emergencies.

Bound the Problem: Resilience plans need to be scoped and bounded appropriately so that executable solutions can be applied and demonstrable progress made. No planning effort can be expected to be effective against every conceivable challenge or in every possible set of circumstances. Planning for resilience needs to recognize that feasibility and resource limitations make it impractical to apply resilience to the entire set of potential targets that might be subject to serious challenges from natural or man-made threats. If there is a policy of fully safeguarding all potential targets, then no targets will be adequately safeguarded. Even with prioritization, planners need to avoid the danger of overextending plans to the point where they are impractical. There need to be risk-informed guidelines for prioritizing such efforts over time in terms of threats and vulnerabilities as relevant to systems, sectors, regions, and communities.

Tailor Solutions: Practical planning for resilience needs to reflect the imperatives stemming from the relevant system's operating and strategic environments as well as its life-cycle status. For each of these contexts, resilience planning processes are most effectively conducted at the earliest stage practicable of a system's life cycle, which is the best stage for incorporating resilience ways and means into critical systems (both human and technical) and their key functions. Applying resilience at the inception stage in the life of every system and function is not always possible, however. The societal, economic, and governmental areas of American life are filled with a vast array of existing systems, incorporating both hard (technical) and soft (human) features, many of which have been in place for long periods and may have become unacceptably vulnerable and brittle in that time. In these instances, as suggested above, best efforts are needed to reduce risk by retrofitting or upgrading these older assets with resilience-consistent features or qualities.

Enhance Coordination: To develop useful resiliency planning processes, enhanced approaches are needed that build on current interagency and intergovernmental mechanisms for coordinating critical infrastructure protection planning to ensure that these usefully connect with and account for the other interagency and intergovernmental planning processes for supporting the homeland security missions. Interagency and intergovernmental planning mechanisms also need to be expanded, where necessary, in terms of their inclusiveness so that they span the stakeholders that represent all levels of the U.S. homeland security enterprise (federal, state, local, tribal, and private sector). Given the scarcity of resources, it is likely that collaborative processes will need to be developed if resilience ways and means are to be practically incorporated across the homeland security enterprise.

Ensure Executability: All plans need certain features and information content in order to be executable. Resilience plans are no different. Tactical, operational, and strategic plans

for activities associated with achieving the resistance, absorption, and restoration end states need to provide for delineation of roles, missions, key relationships, objectives, schedules, and measures or metrics of success. Priorities need to be set and resources made available.

Test Outcomes: Planning solutions need to be tested, practiced, and evaluated through reviews and exercises using a full range of scenarios. While it may seem unusual, special attention needs to be paid to rehearsing the adaptability inherent in resilience, not only on how to deploy and exploit a fixed set of measures. To ensure that resilience plans can be effectively executed also critically depends on the exercise of required capabilities and capacities. Such drills need to be conducted in close coordination with established prearrangements to ensure that they are effectively carried out and their desired results are achieved.

4.2 Planning Against Elements of Resilience

On a more focused level, effective residence planning needs to be attuned to the *objectives o*f resilience, responsive to its *principles,* and capable of applying appropriate ways and means across the *mission spectrum*. How to plan against each of these elements is discussed below.

Objectives of Resilience

To be meaningful, resilience plans need to reflect the three objectives of *resistance, absorption,* and *restoration.* These desired end states provide the essential purposes and the foundation for organizing the logic that plans must have to be effective. They provide critical means of managing complexity by helping planners filter the many variables in a complicated environment to identify those most relevant to intended outcomes. Planning against these objectives also provides a basis from which to make rational decisions regarding the proportion of attention that relevant variables deserve, and to discover cost-effective means of applying resources to fund solutions.

Understanding these objectives is indispensable to the ability to formulate meaningful measures of how well the desired end states have been achieved—an essential element of sound planning. We suggest some basic questions to consider when thinking about this issue, considering each objective in turn:

- Given the application of all identified *resistance* solutions, to what extent have these succeeded in limiting the potential of the threat or hazard at hand to deliver harm, destruction, or loss of national significance against any critical system and its key functions? To what extent does the candidate solution serve to cost-effectively limit the potential damage associated with a particular threat or hazard?
- Assuming application of all identified *absorption* solutions, to what degrees have targeted systems effectively contained and reduced any consequence effects manifested as a result of a damage event and swiftly responded to maintain their key functions at acceptable levels? To what extent do various solutions enable a system to withstand severe internal and/or external stresses and maintain key functions even as it degrades gracefully?

- Given the aggregation of all solutions, to what extent has *restoration* been accomplished? Has any degradation accrued by a critical system been restored? Have the effects of cascading effects been limited? How rapidly have its key functions been reconstituted and reset and its essential wholeness restored?

In seeking to satisfy all three end states, two special needs to be considered. First, that these objectives are interrelated and mutually reinforcing in assuring that a system indeed becomes resilient. Second, the prospect that an optimal solution for meeting one of the resilience objectives might conflict with or tend to reduce the effectiveness of solutions chosen to support either or both of the other two.

Principles of Resilience

The eight principles of resilience discussed earlier not only illuminate the meaning of resilience, but make up a set of criteria that can be used in planning. The presence of features reflecting each principle or characteristic within a particular system is necessary to render it effectively resilient. The lack of one or more principles will create weaknesses that can eventually be exploited by a human adversary in designing an assault or exposed by an extreme natural hazard event when it arrives. For example, a system that is designed and resourced to depend solely on robustness may be costly to produce and ultimately ineffective in defending its critical functions against a manifest threat that is greater in scope, scale, and quality than the worst expected case. In the event that the system's robustness features are overwhelmed, its critical functions will be left exposed to potentially fatal levels of damage with little likelihood of timely rescue or remedy.

The criteria are particularly useful when exploring candidate ways and means intended to produce practical resilience results when applied across the mission spectrum. They can be framed as questions:

- To what degree does the alternative being examined promote adaptability? How cost-effectively does it enable a resilient system to maintain equilibrium when anticipating a damage event or to return to an equilibrium state after experiencing unanticipated adversity?
- In what way does the solution being considered address risk as a function of TVC identified for the system of interest and its key functions? To what stages of the life cycles of expected adverse situations does the alternative apply?
- Are planning solutions accounting for both the soft and hard aspects of resilience, as appropriate? Is there recognition that all critical systems and key functions within the societal, economic, and governmental areas are inextricably linked?

The principles address the all-important need for risk-informed assessments in connection with resilience. Such assessments entail employing a risk method with TVC inputs as a means of informing investment decisions on how resources can be best allocated in incorporating resilience solutions into the key functions of critical systems.

> ***Inputs to Risk Methods:*** Risk methods need TVC inputs not just for the present, but looking toward the future. Developing assumptions on the level and types of threats that systems might face is an essential first step. In terms of future natural disasters, historical data can be extrapolated with some adjustments to provide the threat assumptions needed

to assess risk. Terrorist threats, where reliable and repeatable data is not available, cannot credibly be predicted, but analytically based planning assumptions can be elicited for use in risk assessments. Such assumptions should not focus entirely on extreme worst-case (catastrophic) situations with very low likelihoods of occurrence but with extremely high consequences were such an event to occur. Planners should also posit more realistic yet serious "plausible worst case conditions," more likely to occur and with significant consequences, especially if the frequency of occurrences is high. Risk assessments to assist in finding resilience solutions also need to analyze potentially effective countermeasures across the mission spectrum that can bring resilience ways and means to bear in meeting anticipated threats across the mission spectrum. This means understanding and prioritizing our vulnerabilities, including associated connections and interdependencies.[42]

Allocating Resources: A proper risk assessment helps to ensure that resources devoted to meeting resilience needs provide a substantial and positive return on investment, even where modest amounts are committed.[43] This requires a balanced and comprehensive approach, seeking to obtain the best Return on Investments (ROIs) in resourcing ways and means to ensure that key functions of critical systems are sufficiently resilient. This would entail estimates and trade-offs of how alternative resilience-related solutions that might be incorporated into the prevent, protect, response, and recover mission spectrum against a range of potential terrorist and natural threats can contribute to lowering risks in areas where the existing risk is judged to be too high. An approach to resource allocation that follows this construct is the Risk Assessment Process for Informed Decision-making (RAPID) being developed by DHS to influence program investments in the context of the annual Planning, Programming, Budgeting, and Execution (PPBE) cycle.[44]

Homeland Security Mission Areas

The range of ways and means potentially applicable to resilience requirements is very large. Consequently, it is necessary to rationally group and sort these items in terms of what they do and what purposes they serve, with special attention given to ways and means of supporting resilience objectives. In addition to the criteria discussed above, another important way to help rationally choose among alternative ways and means is to understand them in the context of the homeland security missions of prevent, protect, response, and recover, as discussed earlier.

Experience in providing capability solutions to support the homeland security missions provides a menu of homeland security policies, programs, and activities that can be reviewed by resilience planning. These can be tailored and interpreted as necessary to satisfy resilience objectives in general and more specific resilience needs dictated by their own situational needs and the

---

[42] For a discussion of the elements of risk assessment, see Homeland Security Institute, *Risk Analysis and Intelligence Communities Collaborative Framework*, Final Report, especially the "Risk Tutorial" found in the companion CD, Arlington, VA, April 23, 2009. This document records the results of a study prepared for the Department of Homeland Security, Office of Science and Technology.

[43] Jeff Gaynor, "Infrastructure from a Private Viewpoint," interview with *Defense Management Journal* (UK), March 2007; http://www.defencemanagement.com/feature_story.asp?id=7463.

[44] See U.S. Department of Homeland Security, Risk Management and Analysis (RMA), *Fact Sheet: RAPID II*, July 2009.

operational and strategic environments that bound their areas of responsibility and define the systems relationships for which they need to account.

In planning for resilience in connection with the homeland security missions, it is important not to focus attention on hard elements at the risk of overlooking soft elements. To be relevant and effective, resilience initiatives need to directly address activities and capabilities essential to supporting and maintaining the web of human relationships within communities that are necessary to the resilience of both society and infrastructure.

4.3 Contrasting Resilience Profiles

Planners can profitably use resilience profiles to visualize the desired outcome in the system resilience behavior they seek to achieve though cost-effective investments. The two contrasting examples below illustrate the profiles of two generic system functions that differ markedly in terms of the three parameters of *function*, *latency limit*, and *minimum performance boundary*. In one case, these parameters are set to reflect a stringent resilience standard. In the other case, these parameters are set to a more relaxed standard. The difference in these two examples lies in the varying significance of the roles they perform and the number of connections they have to other systems. Accordingly, each is rationally designed to provide a level of resilience sufficient to its mission, reflecting cost-effective solutions to different problems. This distinction is illustrated by the differently-shaped function performance curves shown in their respective resilience profiles. Both situations are examined with the simplifying assumption of common time and performance scales or dimensions.

Stringent Resilience Profile

The first example, Figure 4 (below), shows a high-gravity system function. While this is intended only to illustrate a generic line-of-business function, practical examples might include a civilian power company's production of electricity, a city government's conduct of local law enforcement activities, or a charity organization's delivery of meals to families living below the poverty line. A resilience profile for any such high-gravity function, being a means of illustrating its desired behavior within a critical system when confronted with a specific threat or hazard, will reflect a short latency limit and a minimal degradation in performance. The tightly constrained character of these parameters reflects the critical nature of the function's role. If the function is allowed to fail, then grave consequences can be expected not only for its host system, but also for the large number of entities to which it is connected or which are dependent on it.

In Figure 4, the threat or hazard that affects the function is also generic, but it could represent a wide variety of dangers. For example, the electric power company might face a threat of multiple improvised explosive devices (IEDs) from a group of militant right-wing extremists. Alternatively, the city government's law enforcement arm might be confronted by a severe weather event (such as a blizzard) that hampers or precludes its ability to conduct patrols or answer complaints. As a third example, the charity might have to deal with an individual firebombing attack by a political extremist group. In any of these cases, a sound risk assessment reveals that a certain distribution of investment will be needed to acquire the ways and means that provide the necessary capabilities to effectively achieve the three resilience objectives with regard to the threat or hazard at hand.

The pie graph in Figure 4 indicates that this generic profile emphasizes resistance, with 50 percent of available resources being applied to service that end state. Notionally, this could reflect a power company's enhanced use of physical security barriers, stand-off distance, and patrolling guard forces at its electricity-generating plants. In the instance of the city police force, it could represent the acquisition of high-mobility, all-terrain utility vehicles to neutralize the effects of heavy weather on patrol and complaint response operations. With regard to the charity, this allocation of resources to serve the resistance objective could indicate the hiring of a contract security force to ensure the safety of facilities and staff.

In all of these notional instances, the application of capabilities serves the same purpose: to limit the damage potential of human threats and/or natural hazards, thus enabling more effective realization of the absorption and restoration objectives. Because it is unlikely in any of these examples that the capabilities applied to serving the resistance objective will be completely effective, resources proportional to the needs identified in a risk assessment must also be applied to building capabilities that will serve the absorption and restoration end states.

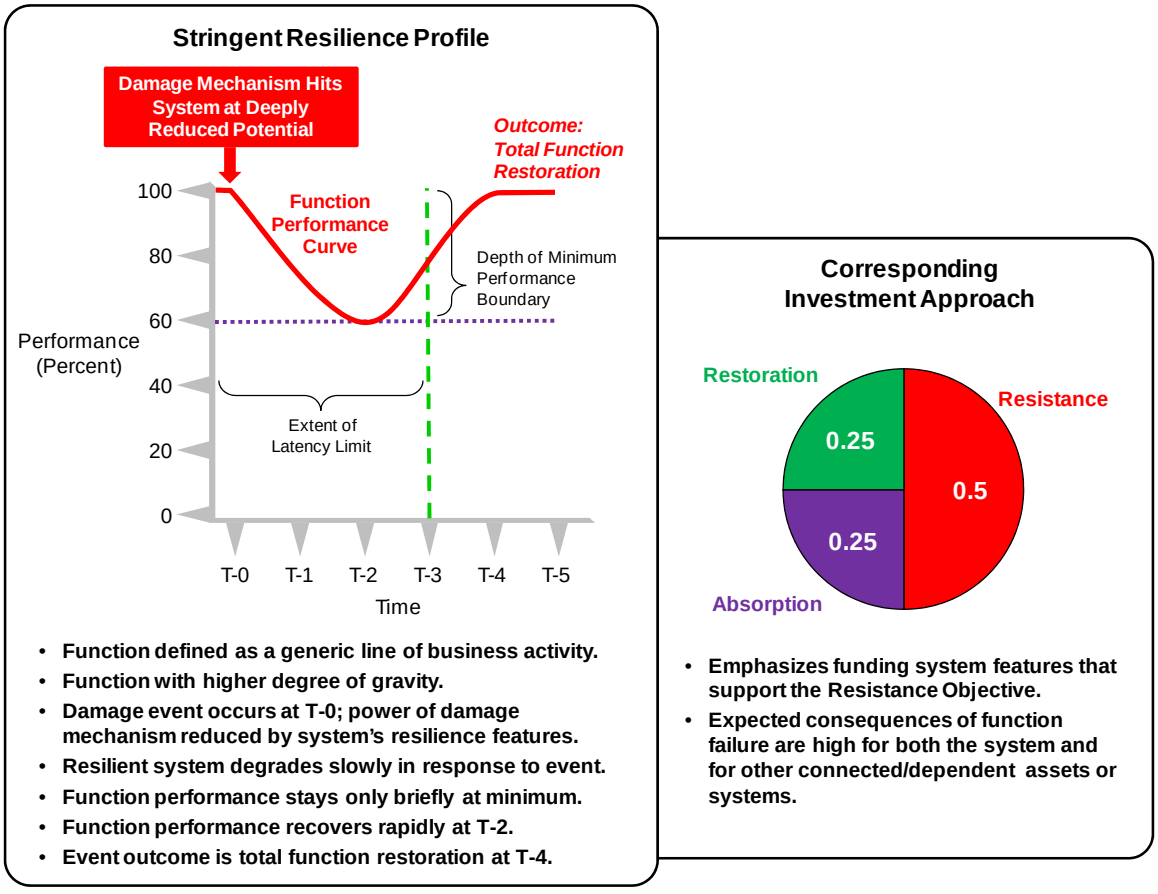


Figure 4: High-Gravity Function of a Resilient System

Relaxed Resilience Profile

The second and contrasting example, Figure 5 (below), shows a low-gravity system function. The graph in this instance also shows a generic line-of-business function. This can serve as a proxy for situations such as a major corporation's recruitment of new employees, the federal

government's operation of national parks, or a major university's basketball program. A resilience profile for any such lower-gravity function will reflect a lengthier latency limit and a substantially lower allowable degradation in performance. The more loosely constrained character of these parameters reflects the more peripheral nature of the function's role with regard to the systems it serves. Even if the low-gravity function is allowed to significantly degrade as illustrated below, serious consequences for the host system and any dependent systems unlikely to accrue.

Figure 5 also includes a generic the threat or hazard that affects the given system function. As with Figure 4, the range of specific examples this could represent is very broad. Situations might include a corporation facing a threat of terrorist small-arms attacks in the countries where its overseas headquarters are located, the federal government's national park system coming under threat from forest fires naturally ignited by increased electrical storm activity, or a university dealing with an earthquake striking its main campus basketball athletic facilities.

As with high-gravity functions, the delineation of resilience profiles for low-gravity functions begins with a risk assessment intended to influence the distribution of investment among the range of solutions that provide necessary capabilities to reach the three resilience objectives. The pie graph in Figure 5 indicates that this generic profile emphasizes restoration, with 75 percent of available resources being applied to service that end state. Notably, the restoration objective can be effectively obtained even if the damage potential of threats or hazards is not greatly attenuated and even if the absorption objective cannot be optimally achieved.

Notionally, this distribution could reflect a corporation's relocation of its headquarters and the residences of its employees to new facilities that incorporate layered physical security measures. In the instance of the U.S. National Park System, it could represent the systematic replanting of burned-over areas with seedling trees. With regard to the major university, this allocation of resources could represent the rebuilding of its basketball center with earthquake-resistant structural features in a less seismically active area. Each of these notional examples shows the application of capabilities to achieve the same aim: to remediate the damaged function by reconstituting and resetting it as is feasible and warranted.

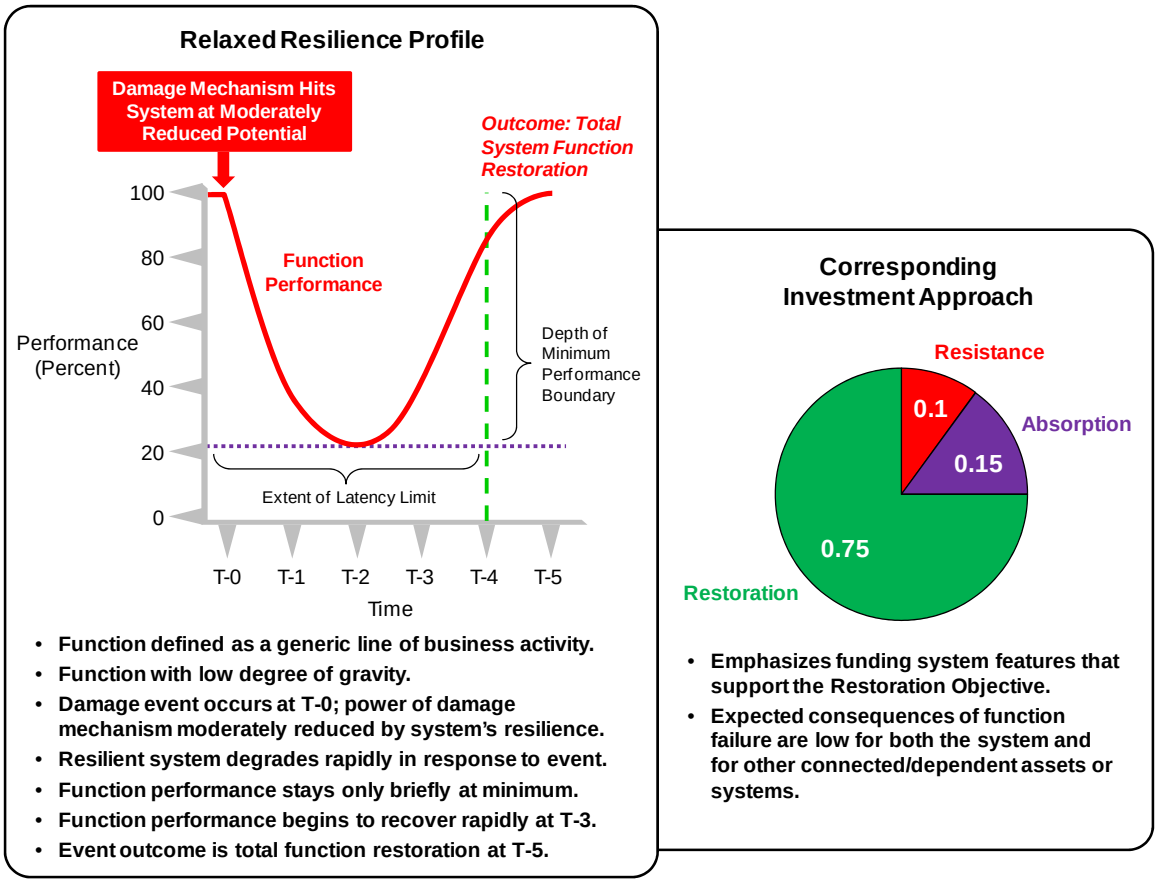


Figure 5. Low-Gravity Function of a Resilient System

This analysis sought to provide a structured framework for moving forward to operationally incorporate resilience into our infrastructure and society. Further analytic work and policy considerations are needed to underpin specific initiatives. We offer suggestions and options in the next section.

5. NEXT STEPS

The purpose of this paper is to present a high-level structured framework for understanding the parameters of resilience, along with a set of guidelines that might be followed in seeking to translate this concept into operational ways and means. If the proposed framework is accepted, many detailed issues need attention before practical steps can be taken to formulate actionable policies, programs, and procedures for incorporating resilience into critical elements of our physical and social infrastructure.

These steps can be divided into three categories, represented by the following questions:

- What specific areas of further analysis might be given high priority with a view towards making resilience truly operational?
- How might DHS assist White House staff in making resilience part of our overall homeland security approach?
- How can stakeholder perspectives on resilience at private and public levels be anticipated and accommodated?

Preliminary suggestions for each of these avenues are provided below.

5.1 Analytic Priorities

One potential area of analytic interest is the question of how to incorporate the resilience construct into various parts of U.S. society, economy, and government so that they actually become more resilient. It is not feasible or wise to attack all parts of this problem at once. Systematic, rational approaches involving risk-informed prioritizing effort offer the prospect of developing an evolving implementation "roll-out" strategy for prioritizing such efforts over time according to critical systems, sectors, regions, and communities.

A second line of possible investigation might be to flesh out in detailed ways the concept of creating resilience profiles to identify systematically the acceptable parameters that each key function within a critical system must demonstrate when it is challenged. This, in turn, might trigger more in-depth analyses of the ways and means that can be applied to operationalize resilience across a range of situations and what investments might be considered. Trade-off assessments and analysis of alternatives would be among the techniques employed.

A final area of suggested analysis concerns resource constraints, which will remain severe due to the economic crises being experienced. It seems questionable that state or local governments are likely to favor any new investments in homeland security for resiliency purposes. The federal government's capacity to serve as the main funding source for at least seed money is also doubtful. This leaves the private sector to take the lead in investing in resilience, possibly supported by federal stimuli in the form of tax incentives, targeted grants, and liability coverage. These and other significant issues and possible solutions would form a powerful area of study with the potential for large payoffs in making resilience happen.

5.2 DHS Issues

As the primary agency with homeland security responsibilities and authorities, DHS might usefully consider a number of initiatives that can move resilience forward, responsive to guidance from the new White House Directorate. Initiatives DHS might consider include

- Formulating a preliminary draft policy directive, perhaps a separate Presidential Directive (PD) that establishes the policies, purposes, and parameters of resilience and how it should be incorporated into homeland security planning and preparedness. This would articulate not only the federal level role in resilience but also the reinforcing roles and responsibilities of non-federal stakeholders, both public and private. The draft would provide a set of high-level guidelines for operationalizing resilience in terms of responsibilities, solutions, and investments.
- Reviewing relevant existing implementation documents to determine the extent to which they would require modifications to align themselves with the broad resilience policy statement in order to provide the practical steps needed to incorporate resilience on the ground. Resilience elements in the NIPP could be strengthened and resilience objectives and principles might be inserted into the National Preparedness Guidelines (NPG) and National Response Framework (NRF).[45]
- Developing a plan of action to make the case to each major stakeholder group that resilience is a necessary, feasible, and desirable objective to be attained by using ROI, demonstrating to governments, businesses, communities, and citizens that the benefits in lowering risks of all-hazard threats to the functioning of our economy and society are well worth the costs in dollars, effort, and time. Proactively constructing such a plan is essential, since without such buy-in, resilience cannot be realized in a practical and effective sense.
- Exploring how DHS and the federal government might stimulate the application of resilience at state and local government levels, with nongovernmental organizations (NGOs), and within the business community. Examples of such initiatives are grants, tax incentives, liability protection, and other initiatives. In this connection, one approach that has been discussed is the concept of public-private partnerships to support the development of a more resilient nation.[46]

5.3 Stakeholder Initiatives

While at least preliminary acceptance by all relevant federal agencies is needed for any serious resilience initiatives, the major challenge—if experience is any guide—is in obtaining stakeholder buy-in at the state and local government levels, with NGOs and communities, and across the private sector. This highlights the challenges of achieving coherence in pursuing resiliency in a complex stakeholder environment if federal agencies, their state and local partners, Congress, and

[45] While undergoing revisions and enhancements, the NPG and NRF will remain relevant as doctrinal and operational documents. The latest versions of these documents are referenced in the Bibliography.

[46] For an insightful discussion of building private-sector resilience, see McNeil.

industry choose to oppose likely changes in policies, reallocations of funding, and shifting responsibilities.

Attempts by the federal government to impose resilience will not succeed. Inputs, feedback, and ultimately buy-in from other public stakeholders and the private sector must be sought, however difficult this may be. Before DHS, the White House, or any federal policies on resilience reach a mature level, substantial efforts would need to be made in seeking comments from other significant stakeholders.

Vehicles and venues for obtaining stakeholder feedback can include involving FEMA Regional Administrators to interact with state, local, and private partners, tapping the Government and Sector Coordinating Councils within the NIPP framework, seeking assistance from the National Governors Association, holding focus group meetings with selected representative at the local level, and using business associations.

The above steps will take time, effort, and resources to execute. Resilience means many things to different players across the homeland security stakeholder community, but this need not remain an impediment to moving ahead in a productive direction. It is important to use the opportunity afforded by the Obama Administration's interest in resilience to turn this concept into reality and get it right. If this cannot be accomplished, the concept of resilience will likely not have an operational impact in making the homeland more secure.

BIBLIOGRAPHY

Governmental

Centers for Disease Control and Prevention. *Strategic National Stockpile.* http://www.bt.cdc.gov/stockpile/U.S. Department of Defense. *National Defense Strategy*. Washington, DC, June 2008. http://www.defenselink.mil/news/2008%20national%20defense%20strategy.pdf.

U.S. Department of Homeland Security. *One Mission, Securing Our Homeland; U.S. Department of Homeland Security Strategic Plan 2008-2013*. Washington, DC, September 2008. http://www.dhs.gov/xabout/strategicplan/.

———. *National Infrastructure Protection Plan*. Washington, DC, 2009. http://www.dhs.gov/files/programs/editorial_0827.shtm.

———. *National Preparedness Guidelines*. Washington, DC, September 2007.

———. *The National Strategy for Maritime Security*. Washington, DC, September 2005. www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf.

———. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC, February 2003. http://www.dhs.gov/files/publications/publication_0017.shtm.

———. "Remarks by Secretary Napolitano at the Council on Foreign Relations," released July 29, 2009.

U.S. Department of Homeland Security, Federal Emergency Management Agency. *National Response Framework*. Washington, DC, January 2008. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

U.S. Department of Homeland Security, Homeland Security Advisory Council. *Report of the Critical Infrastructure Task Force*. Washington, DC, January 2006. www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf

———. *Top Ten Challenges Facing the Next Secretary of Homeland Security*. Washington, DC, September 11, 2008. www.dhs.gov/xlibrary/assets/hsac_dhs_top_10_challenges_report.pdf.

U.S. Department of Homeland Security, Risk Management and Analysis. *Fact Sheet: RAPID II*, July 2009.

U.S. Department of Homeland Security, Risk Steering Committee. *DHS Risk Lexicon*, Washington, DC, September 2008.

The White House. *Homeland Security and Counterterrorism.* http://www.whitehouse.gov/issues/homeland_security/.

———. *The National Security Strategy of the United States of America*. Washington, DC, March 2006. http://georgewbushwhitehouse.archives.gov/nsc/nss/2006/.

———. *National Strategy for Combating Terrorism*. Washington, DC, September 2006. http://georgewbush-whitehouse.archives.gov/nsc/nsct/2006/.

———. *Presidential Policy Directive-1*. Washington, DC, February 13, 2003.

The White House, Homeland Security Council. *National Strategy for Homeland Security*. Washington, DC, October 2007. http://www.dhs.gov/xabout/history/gc_1193938363680.shtm

Nongovernmental and Academic

Allenby, Brad, and Jonathan Fink. "Toward Inherently Secure and Resilient Societies." *Science*, vol. 309, no. 5737 (August 12, 2005): pp. 1034-1036.

Arnold, Mary. *The Resilient Homeland: Broadening the Homeland Security Strategy* (testimony before the House Committee on Homeland Security). May 6, 2008.

Barabasi, Albert-Laszlo and Bonabeau, Eric. "Scale-Free Networks." *Scientific American*, vol. 288, no. 5 (May 2003): p. 60.

Birkland, Thomas A. "Disasters, Catastrophes, and Policy Failure in the Homeland Security Era." *Review of Policy Research*, vol. 26, no. 4 (2009): pp. 226-227.

Carafano, James Jay. *Backgrounder: Resiliency and Public-Private Partnerships to Enhance Homeland Security*. The Heritage Foundation, Washington, DC, no. 2150, June 24, 2008.

Cascio, Jamais. "The Next Big Thing: Resilience." *Foreign Policy*, vol. 88, no. 3 (May/June 2009).

Colten, Craig E., Robert W. Kates, and Shirley B. Laska. "Three Years After Katrina: Lessons for Community Resilience" *Environment*, vol. 50, no. 5 (September 2008): pp. 36-47.

Elron, Meir. "Israel's Homeland Security Concept: From Civil Defense to National Resilience." Briefing presented to HSsaI, August 4, 2009.

Flynn, Stephen E. "America the Resilient." *Foreign Affairs*, vol. 87, no. 2 (March/April 2008): pp. 2-8.

———. *The Edge of Disaster: Building a Resilient Nation*. New York: Random House, 2007.

Gaynor, Jeff. "Critical Infrastructure from a Private Viewpoint." *Defense Management Journal*, no. 36, (2007). http://www.defencemanagement.com/article.asp?id=249&content_name=Homeland%20Security&article=7463.

George Mason University School of Law. "Critical thinking: Moving from Infrastructure Protection to Infrastructure Resilience." CIP Program Discussion Paper Series, February 2007.

Harvard Business School. "Leadership on 9/11: Morgan Stanley's Challenge." December 17, 2001. http://hbswk.hbs.edu/archive/2690.html.

Homeland Security Institute. *Risk Analysis and Intelligence Communities Collaborative Framework*, Final Report, April 23, 2009. Prepared for the Department of Homeland Security, Office of Science and Technology.

Hsu, Spencer S. "Obama Integrates Security Councils, Adds New Offices: Computers and Pandemic Threats Addressed." *Washington Post*, May 26, 2009, p. 4.

http://www.washingtonpost.com/wp-dyn/content/article/2009/05/26/AR2009052603148.html.

Jackson, Brian A. "Marrying Prevention and Resiliency." RAND Corporation Occasional Paper, 2008.

Horwitz, Steven. "Hurricane Recovery Comes Out of a Box." *Local Knowledge*, no. 1 (Summer 2008): pp. 48-55.

McConnell, Allan, and Drennan, Lynn. "Mission Impossible? Planning and Preparing for Crisis." *Journal of Contingencies and Crisis Management*, vol. 14, no. 2 (June 2006).

Mileti, D. *Disasters by Design: A Reassessment of Natural Hazards in the United States*. Washington, DC: Joseph Henry Press, 1999.

Norris, Fran, et al. "Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness." *American Journal of Community Psychology* (2008): pp. 127-150.

McNeill, Jena Baker. "Backgrounder: Building Infrastructure Resiliency: Private Sector Investment in Homeland Security." The Heritage Foundation, Washington, DC, no. 2184, September 23, 2008.

Olshansky, Robert, and Laurie Johnson. "Improving Post-Disaster Recovery: Initial Thoughts for a New Administration," University of Illinois at Urbana-Champaign and Laurie Johnson Consulting. San Francisco, California, November 17, 2008.

O'Rourke, T. D. "Critical Infrastructure, Interdependencies, and Resilience." *The Bridge* (Spring 2007): pp. 27-29.

The Reform Institute. "Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy," 2008. http://www.reforminstitute.org/DetailNews.aspx?nid=1322&cid=.

Rose, Adam. "Economic Resilience to Natural and Man-made Disasters: Multidisciplinary Origins and Contextual Dimensions." *Environmental Hazards: Human and Policy Dimensions* (2007): pp. 1-16.

Rose, Adam, Ghabedo Oladosu, and Shu-Yi Liao. "Business Interruption Impacts of a Terrorist Attack on the Water System of Los Angeles: Customer Resilience to a Total Blackout," *Risk Analysis*, vol. 27, no. 3 (2007): pp. 513-531.

Sheffi, Yossi. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, MA: MIT Press, 2005.

Wachtendorf, Tricia. "What Is Community Disaster Resilience? Presentation at Building Community Resilience and a Culture of Preparedness." NORAD and USNORTHCOM Surgeon's Conference, March 10-12, 2009.

Wang, Fan Xiao, and Guanrong Chen. "Complex Networks: Small-World, Scale-Free and Beyond," *IEEE Circuits and Systems Magazine* (Spring 2003): pp. 15-16.

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE
2900 South Quincy Street • Suite 800 • Arlington, VA 22206-2233