Resilience Redux: Buzzword or Basis for Homeland Security

Jerome H. Kahan

ABSTRACT

Since 9/11, resilience, a term used widely in many disciplines, has occupied a place in homeland security policy and programs. Peaking in importance as the last decade ended, resilience has begun to retreat as an official driver of U.S. homeland security strategy. Preparedness, which can yield resilience as one of its outcomes, has become the official focus. However, resilience is still used in a variety of ways with different meanings by homeland security officials and in various official documents. Non-governmental experts and institutions have not slackened their efforts to research, write about, and teach resilience in relation to homeland security. The purpose of this article is to demonstrate the ebb and flow of resilience in homeland security policy and investigate the future role resilience might play in homeland security policy.

INTRODUCTION

For many decades, resilience has been a relevant concept in variety of fields, including psychology, sociology, physics, civil engineering, supply chains, economics, business, energy, and ecology.[1] While resilience had for years been applied to aspects of disaster relief such as the impact of earthquakes, the concept of resilience can be said to have officially entered the world of homeland security in response to the tragic 9/11 event.[2] In the years following, a veritable cottage industry on resilience related to homeland security appeared in the academic and research community throughout the nation and across the globe. There have been innumerable workshops, conferences, books, articles, and courses of study dealing with this subject, as well as entire organizations devoted to this topic.[3]

Interest in resilience did not go unnoticed in U.S. government circles. In part responding to a recommendation of the *9/11 Commission* to make our nation "stronger, safer, and more resilient," this concept also gained prominence in U.S. homeland security policy formulation.[4] As the years passed, the White House and the Department of Homeland Security (DHS) have incorporated resilience into homeland security planning processes, implementation programs, and operational activities. Employed both conceptually and on limited operational levels, resilience can be found in such significant homeland security documents such as the first and second *Quadrennial Homeland Security Reviews (QHSR)* and the *National Preparedness Goal (NPG)*.[5]

Wide use of resilience in connection with homeland security does not mean there has been agreement on the definition of this term. President Obama offered a generalized meaning of resilience expressed broadly as "the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies."[6] However, the governmental and academic homeland security communities have not adopted this or any other single definition as the agreed meaning of the term. Innumerable variations of definitions abound, depending upon the needs and perspectives of the definer.[7]

This article seeks to investigate whether resilience should not only continue to serve as a broad concept in U.S. homeland security strategy, but, more importantly, whether it can become a realistic basis for operationally–oriented policies and programs as the nation faces increasingly challenging threats and hazards. Among the issues addressed are:

- The nature and scope of resilience definitions.
- Challenges in operationalizing resilience.
- Resilience in U.S. homeland security policy.
- The future of resilience in homeland security.

Meaning of Resilience

Considerable attention has been paid to finding a definitive meaning of resilience to apply to various aspects of homeland security.[8] Relatively standard sets of meanings for resilience can be found in more mature fields such as physics, psychology, sociology, and even environmental science. As illustrated below, there is little if any agreement in government or academic circles on the meaning of resilience as applied to homeland security.

Spectrum of Definitions

In its broadest sense, resilience in the world of homeland security has to do with people, communities, institutions, and infrastructure experiencing an adverse incident or series of incidents, withstanding such blows, and returning to functionality. The following paragraphs present a series of terse statements about resilience. Taken together, they tell a relatively complete story of resilience as related to homeland security—its purpose, principles, and parameters.[9]

- Resilient systems are flexible and adaptable, unlike brittle systems that can break when undergoing natural and man-made hazards. Such systems can absorb disturbance, degrade gracefully, and bounce back to resume functioning. More resilient targets are potentially less susceptible to disruption, and therefore of lesser interest to terrorists.
- Resilience ensures that a system can continue to function at a certain critical minimum level during and in the immediate aftermath of a disruption. These systems can withstand impacts, restore functioning to the pre-incident level, return to a lower but acceptable level of functionality, or potentially come back to an even more resilient posture.
- Resilient systems can deal with the unexpected through flexibility and ingenuity. They apply extra effort or take adaptive actions that go beyond the inherent ability of a system to withstand adverse incidents. They can undergo change, learn from disasters, and improve their resilience as result of experiencing major disruptions.
- Resilience provides system capabilities to recover from both the initial impact and the potentially cascading consequences of a series of undesirable events. However, the reach of resilience as a characteristic of a system is relevant across the full set of homeland security missions, including prevent, protect, and mitigate, not only to disaster response and recovery capacities.[10]
- Resilience is a holistic, integrated, and synergistic process of evolving end states, whereby adaptive capabilities continually improve the level of functioning. It is a "dynamic capability" that responds to and anticipates changes in the operating environment, matures over time, and is integral to systems operations and culture.

Two additional points should be mentioned. First, resilience is *not* equivalent to preparedness. Instead, it serves as an *outcome* of preparedness – a term signifying the range of activities that public and private homeland security stakeholders undertake to enhance their ability to effectively deal with threats and hazards they might experience.[11] Second, resilience in the homeland security context is *inversely* related to risk. As the resilience of a system increases, the risks it faces due to adverse events will tend to decrease.[12]

Resilience within Domains

The resilience story has another chapter, however. According to a comprehensive study of how resilience has developed over the past decades, while this concept is by nature interdisciplinary, applications have tended to fall into discrete fields or domains.[13] Numerous suggestions have been offered for how to formulate the most useful set of domains when applied to homeland security.[14] The author favors a five-part set composed of individuals, infrastructure, institutions, ecosystems, and communities.[15]

Individuals

This domain applies to individuals who experience stressful conditions of all kinds. Resilience in this context means the capacity of such individuals to withstand such experiences and recover as rapidly as feasible to a state of personal well- being and social and professional functioning.[16]

Infrastructure

This domain encompasses engineered assets, systems, and networks, whether physical or cyber. Resilience applied to physical systems entails technical and structural improvements that enable "hard" systems to withstand adverse events without functional failure and rapidly return to a level of acceptable functionality. More sophisticated computer-based actions are needed to enhance resilience of "soft" cybersysytems.[17]

Institutions

This includes social organizations, for profit and non-for profit enterprises, businesses, corporations, as well as government departments and agencies. Emphasis tends to be placed on continuity of operations and flexibility.[18]

Ecosystems

This domain covers living organisms and their physical environment. A unique aspect of a resilient ecosystem after receiving a disruption is its capacity to adapt and change to different configurations within its inherent "state of being."[19]

Communities

This involves finding balanced measures that can improve the overall ability of a community to withstand threats and hazards, continue to function, and return to a state of well-being. Given that a community is a mixture of individuals and societal elements, as well as relevant infrastructures, institutions, and ecologies, attaining resilience in this domain is very challenging.[20]

The absence of a common understanding of how to define resilience suggests that there is no easy one-size-fits-all approach for applying resilience in connection with homeland security issues. Arguments have been made for establishing a common definition of resilience for all users and for all purposes.[21] However, this does not seem feasible. Moreover, a variety of definitions has the benefit of providing users with flexibility in applying resilience in differing situations.

Users can examine the definitions and interpretations of resilience offered above, or hunt for more, in order to discover the best way of defining this concept for their purposes – whether planning to make a system more resilient or improving the resilience of a system in being. For users preferring a more analytic approach, DHS's Homeland Security Studies and Analysis Institute (HSSAI) developed a structured framework that would allow users to select the basic definitional option best suited to their needs, given types of human or naturally caused threats, hazards, or disruptions faced by the system and the domain it occupies.[22]

The author appreciates the fact that a diverse set of resilience meanings exists and might have value over a common definition. On the other hand, if pressed to characterize

the meaning of any system in any domain "behaving resiliently" in the face of any adverse incident, the author would define this as its ability to "absorb stress or destructive forces through resistance or adaptation, manage or maintain basic functions and structures during disastrous events, recover or 'bounce back' after an event, and experience minimum disruption … after a hazard event has passed."[23]

Operationalizing Resilience

A number of years ago, a distinguished economic expert with no homeland security expertise wrote "Resilience is in danger of becoming a vacuous buzzword from overuse and ambiguity…"[24] However, turning the concept of resilience into operational programs is not an easy task. Early initiatives to insert resilience operationally into homeland security activities and actions were aimed at safeguarding U.S. infrastructure. More recent efforts center around finding ways to turn the Quadrennial Homeland Security Reviews (QHSR) into realistic actions and operational programs.

Where Are We?

During the latter part of the last decade, the notion of Critical Infrastructure Protection (CIP) began to give way to the idea of Critical Infrastructure Resilience (CIR).[25] The National Infrastructure Advisory Council (NIAC) has produced studies on encouraging DHS "to provide each critical infrastructure sector maximum flexibility to develop and adopt resilience strategies that match their operating model, asset base, and risk profile," and has generated case studies designed to set sector-specific resilience goals, starting with nuclear energy and electricity.[26] Further work has focused on improving infrastructure resilience on a regional basis.[27] The DHS *National Infrastructure Protection Plan (NIPP)* has paid increasing attention over the years to resilience as a concept for securing the nation's critical infrastructure and key resources (CI/KR) including cybersystems.[28]

In the realm of community resilience, The Community and Regional Resilience Institute (CARRI) has for many years sought to develop processes for communities to move ahead in enhancing their resilience. Finding effective and acceptable methods for assessing resilience in a community context, however, has continued to present major challenges, not only from an analytical standpoint, but also from the standpoint of incentivizing community leaders to invest in strengthening their resilience. Pilot programs to address this issue have continued.[29] The Community Resilience Task Force (CRTF), overseen by DHS's Homeland Security Advisory Committee (HSAC), observed in a June 2011 report observed that many homeland security activities are already underway, but "those activities are rarely linked explicitly to resilience."[30]

On a more generalized level, in late 2011, a George Washington University Homeland Security Policy Institute (HSPI) Task Force called on national policymakers and homeland security practitioners to move beyond the conceptual discussion of resilience and advance practical and tangible means to realize resilience aims.[31] With little amplification, this task force recommends painting a presumably practical "picture of a resilient nation" by applying a "systems-based approach that emphasizes risk management practices as a unifying theme for resilience policy…combining separate disciplines of mitigation, preparedness, response, and recovery, into a continuum of resilience."[32]

From another perspective, that of missions rather than domains, a 2012 National Academy of Sciences (NAS) Report concludes that "resilience has assumed heightened importance as a homeland security concept, especially as natural disasters have become more damaging".[33] While calling for incorporation of national resilience as a strategic principle and discussing issues of performance metrics and other analytical challenges, this report only addresses how to increase resilience to disasters with emphasis on response and recovery. Limiting resilience to planning for disaster response and recovery, however, falls short of viewing resilience as an overarching construct for homeland security covering *all* homeland security missions. This is needed if resilience

is to become a practical strategic guidepost for homeland security planning, policymaking, and program formulation.

Resilience capabilities cannot be incorporated when disaster strikes, but need to be planned and implemented as part of preparedness at the national and local level. Planning for implementing the concept of resilience in practical ways needs to account for the fact that resilience encompasses "hard" systems (such as infrastructure and assets) as well as "soft" systems (such as communities and individuals).[34] One useful approach for planning resilience applications is to establish a "resilience profile" depicting how the operational performance of a given system would be affected by various hazards and how this performance profile can be improved by investments that incorporate resilience capabilities into the system's features.[35]

In planning for resilience, readers need to be aware that not all systems can or should be designed to be resilient, considering their purpose and threat environment. For example, if a circuit breaker is resilient to a large power surge, it may resist shutting down power, with adverse consequences to the system.[36]

Measuring Resilience

Without a credible and pragmatic assessment tool for measuring resilience, turning this concept into real, cost-effective policies and programs does not seem possible. As in the case of definitions, the question of how resilience can be measured has also been addressed by a relatively large number of sources offering a wide variety of approaches, with a comparable lack of agreement on this issue as well.[37]

In a recent report the GAO recommended that homeland security officials "develop performance measures to assess the extent to which asset owners and operators [...of infrastructure systems] are taking actions to resolve resiliency gaps identified during the various vulnerability assessments."[38] In response, the department noted that efforts towards this end have already been initiated, with new performance metrics for critical infrastructure resilience under review.[39] Efforts to develop such measures are being undertaken within DHS, specifically by S&T.[40]

The *HSSAI r*eport mentioned above offers an approach for developing measures and metrics associated with various meanings of resilience for a given threat scenario. Again, the infrastructure domain represents the best domain for measuring resilience. An example of such a measure is how well a production system behaves in limiting its loss of functionality after encountering a disruption, with metrics including "the rate and amount of inputs, throughputs, or outputs per unit of time."[41]

As suggested above, progress has been made in measuring the resilience of critical infrastructure elements that are technical and structural in nature. When it comes to community resilience, for example, this issue has been raised repeatedly, though finding credible performance measures has been far more challenging.

- The CRTF task force calls for DHS to coordinate development of a "community-based, all-hazards American Resilience Assessment (ARA) methodology and toolkit," presumably including steps to measure needs and progress.[42] It is unclear whether DHS has acted upon this recommendation.[43]

- The NAS report calls for community-driven and top-down resiliency measures, which are relevant to meaningful assessment methods. This would be an extremely complex undertaking, and it appears that there has been no follow- up by the academy.

- CARRI has sought to understand the complex issue of measuring performance in connection with community resilience. However, it does not appear that the needed range of effectiveness measures has yet been developed for operational use, given the public policy as well as analytical challenges in doing so.

A comprehensive study by Argonne National Laboratory rigorously demonstrates the many challenges of finding a credible measurement method for community resilience. As the study points out, "The methodology required to

capture resilience at the community/regional level is very complex and will involve not only surveys of individual assets but discussions with stakeholders, identification of critical community and regional capabilities, and identification of interdependencies among these entities."[44]

Before turning to how the government has handled resilience, the following observation by an academic expert on community resilience remains as valid today as it was a few years ago.

> The idea of building resilience to natural and man-made disasters is now a dominant strategic theme and operational goal in the current U.S. national security policy discourse.... Researchers in varied and distinct disciplines have struggled with the concept of *resilience* in their respective fields for decades. Scholars and practitioners continue to wrestle with this concept in hope of developing useful prescriptive homeland security policy guidance, and community-level assessment tools. While there is still much to debate about how to draft precise definitions of resilience and its attributes, and how to *operationalize and apply resilience concepts within each discipline*, overlap in the research of each discipline is significant enough to be instructive as to what makes systems resilient.[45]

Resilience in U.S. Homeland Security Policy

In a speech celebrating National Preparedness Month in 2009, President Obama reminded the nation that the concept of resilience "is not new, and different eras in our history reflect an unwavering focus on building national resilience."[46] In more recent times, stimulated by the threat of terrorism and a spate of high consequence natural disasters, resilience has been a central concept in U.S. homeland security policy. It has to varying degrees and with differing interpretations, found its way into major strategy and planning documents issued by the White House and DHS. It has also been applied to a number of highly specific initiatives. Efforts to operationalize this concept have been moving forward, but doing this fully and successfully has been challenging.

Resilience as a National Strategy Concept

The concept of resilience did not immediately become part of the official lexicon of homeland security as part of the nation's reaction to 9/11. It was not mentioned in President G. W. Bush's dramatic speech that highlighted the dangers of international terrorism and how we will fight this threat and not let it harm our freedoms and way of life.[47] Nor was resilience mentioned in connection with the missions for the establishment of the Office of Homeland Security (OHS), which was given responsibilities for coordinating executive branch efforts "to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."[48] As it was being disbanded in 2002 to make way for the creation of DHS, OHS produced the first N*ational Strategy for Homeland Security (NSHS)*.[49] However, this significant first- of- its-kind strategic document for homeland security did not mention the concept of resilience either.

The devastation caused by Hurricane Katrina in 2005 led to harsh criticisms of how the federal government, as well as state and local governments, handled this situation. Given that catastrophic natural disasters such as Katrina cannot be prevented, a far more efficient and effective set of capabilities and policies for response and recovery must be instituted. To improve federal level management of major disasters, the *Post Katrina Emergency Reform Act (PKERA)* reorganized FEMA by making it an operational component within DHS, with wider responsibilities for federal level preparedness and the ability for the administrator to report directly to the Secretary of Homeland Security and also to the president. Its missions were given as response, recovery, and mitigation as well as protection, but there was no mention of resilience.[50]

The second edition of the *NSHS*, issued by the Homeland Security Council in 2007, represented a major step forward in producing a comprehensive homeland security strategic

document that incorporated resilience as an element of safeguarding critical infrastructure of communities, including such elements as communications, supply chains, transportation systems, and cybersystems against major terror attacks or natural disasters.[51] While a major step forward in embedding resilience in official policy, this document did not discuss resilience as applicable to domains other than critical infrastructure.

In early 2008, the DHS *Five Year Strategic Plan* was issued, with the Secretary of Homeland Security characterizing the American people as resilient and putting forth his vision for the security of the homeland as "a secure America, a confident public, and a strong and resilient society and economy."[52] In that same year, Congressional interest in resilience led to a series of hearings by the Homeland Security Committee of the U.S. House of Representatives. In this connection, the committee chairman declared May 2008 as "Resilience Month."[53]

Tracing the rising trajectory of resilience suggests that the year 2010 represented a high point in the significance of this concept in homeland security policy. In that year, President Obama's 2010 *National Security Strategy (NSS)* explains,

> We will not be able to deter or prevent every single threat. That is why we must also enhance our resilience. When incidents occur, we must show resilience by maintaining critical operations and functions … [while] adapting to changing conditions, and prepare for, withstand, and rapidly recover from disruption… returning to our normal life…[54]

One month later, the first *QHSR*, a document of major significance for DHS and the HSE as a whole, highlighted to Congress and the nation the need for resilience – taken to mean "fostering individual, community, and system robustness, adaptability, and capacity for rapid recovery."[55] The *QHSR* included resilience as part of the "vision" of " *A homeland that is safe, secure, and resilient against terrorism and other hazards, where American interests, aspirations, and way of life can thrive."*[56] The document then goes on to identify resilience as one of "three key concepts that are essential to, and form the foundation for, a comprehensive approach to homeland security." It also makes certain that readers fully understand that the president is "uniquely responsible for the safety, security, and resilience of the Nation."[57]

Also in 2010 President Obama signed *Presidential Policy Directive -8 (PPD-8)*, an initiative aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters. The directive employs a definition of resilience as "the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies."[58] The associated *NPG*, issued in 2010, states its purpose as producing "a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."[59]

Continuing to put priority on resilience for critical infrastructure, last year a presidential policy directive established "a risk-informed approach and a framework for critical infrastructure security and resilience collaboration."[60] In this same year, a presidential executive order set policy on cyber threats to critical infrastructure.[61] With the bulk of US infrastructure in private hands, public-private partnerships are said to "advance the security and resilience of critical infrastructure under the National Infrastructure Protection Plan."[62]

Bringing us up to date, the second *QHSR,* recently issued, does not repeat all the points in the first edition on resilience. However, it does refer to the *NPG* purpose of ensuring "[a] secure *and resilient* nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."[63] Continuing along this line, this *QHSR* goes on to say, "in this manner, *national preparedness increases security and resilience by helping our Nation systematically prepare for the threats and*

hazards that pose the greatest risk."[64] Through these references, the second *QHSR* seems to be making a deliberate effort to ensure that readers are aware of the importance of the *NPG* and the overall *PPD-8* preparedness effort, which is focused on operational-level homeland security preparedness activities, as discussed below. However, it still treats resilience in more of a generalized rather than operational manner.

Resilience on an Operational Level

As discussed earlier, headway has been made relatively early in operationalizing resilience in connection with making critical infrastructure systems "more reliable, efficient, and resilient" by designing in "cost-effective security and resilience features."[65] One of the more operationally oriented objectives of the DHS Fiscal Year 2008-12 Strategic Plan is to "Protect and Strengthen the Resilience of the Nation's Critical Infrastructure and Key Resources".[66] This and the growing inclusion of resilience as a homeland security concept stimulated the *Homeland Security Studies and Analysis Institute (HSSAI)* to produce a study on an Operational Framework for Resilience, which was cleared for public release and published in a homeland security journal.[67]

Towards the end of his first term, pressure was put on the Obama Administration to operationalize resilience by a number of distinguished non-governmental groups. An HSPI Task Force concluded in 2011, "The White House and the Department of Homeland Security (DHS) must advance U.S. capacity for resilience or else a loss of momentum will result in resilience being little more than a buzzword."[68] At about this same time, a senior DHS official reportedly asked, "How do we operationalize resilience every day as part of the work that we do?" The official acknowledged that "little is being done …to make it happen," [… but claimed] "that's something… DHS is trying to change."[69] The GAO in 2012 pressed DHS to go beyond just a resilience framework and develop an implementation strategy that includes "steps needed to achieve results, by developing priorities, milestones, and performance measures; responsible entities, their roles compared with those of others, and mechanisms needed for successful coordination; and sources and types of resources and investments associated with the strategy, and where those resources and investments should be targeted."[70]

Other strategic documents have begun to focus on operationalizing the concept of resilience. Of special significance is the first *QHSR*. In addition to making resilience a prominent concept, this document also treats resilience operationally in connection with the mission of *Ensuring Resilience to Disasters* through rapid recovery from natural disasters or terrorist attacks.[71] Resilience is explicitly associated with one of the specific goals of the Cybersecurity Mission, but does not appear as part of other goals for the remaining missions.[72] The second *QHSR*, reaffirms the relevance of resilience to the operational mission of *Ensuring Resilience to Disasters*, but does not apply this term in connection with other missions or associated goals, as found in the first edition.[73]

The *NPG* has much to say about resilience in connection with the set of preparedness "core capabilities." Core capabilities are designed to support the full spectrum of homeland security operational missions – prevent, protect, mitigate, respond, and recover. To varying degrees and depending upon circumstances, most of these core capabilities, when incorporated into the various systems that together comprise the nation— communities, citizens, government entities at all levels, private and not-for-profit organizations, buildings, transportation systems, businesses, institutions, cybersystems, and ecosystems— have the effect of providing them with the ability to "behave resiliently" when experiencing major disruptions.[74]

The following discussion summarizes how incorporation of preparedness core capabilities can directly or indirectly contribute to the resilience of whatever system is being endangered. To begin with, there are three core capabilities common to all missions, all of which explicitly include resilience.[75]

- Prior planning for resilience includes drills to instill in communities and businesses the concept of thinking and acting flexibly and creatively in the event of a disaster.
- Public information can explain the basic resilience concept of "bending but not breaking" when an adverse event is experienced and techniques for enabling such reactions.
- Operational coordination can support resiliency if it includes options for adapting to the impact of a disaster by finding ways to maintain the essential coordination needed to effectively cope with such a challenge.

Secondly, resilience features and measures are implicit in most of the core capabilities associated with prevent, protect, respond, and recover missions.

- *Prevent* core capabilities and objectives are aimed at identifying thwarting, intercepting, redirecting, or at worst lessening the impact of threats posed by intelligent adversaries. If a lessened impact is experienced, resilience will be less stringent, and improvements will enable the impacted entity to maintain key functions, become stable, and rapidly restore its performance.
- *Protect* capabilities focus on actions to protect the citizens, residents, visitors, critical assets, systems, and networks against the greatest risks to our nation, creating conditions for a safer, more secure, and more resilient nation.
- *Response* capabilities seek to ensure the resilience to effectively respond to any threat or hazard, saving and sustaining lives and stabilizing the incident, as well as rapidly meeting basic human needs, restoring basic services, establishing a safe and secure environment, and supporting the transition to recovery.
- *Recovery* capabilities support resilience in restoration of a community's physical structures as well as providing a continuum of care to support physical, communications, health, safety, psychological, and emotional needs of the community, including response and recovery personnel.

Thirdly, resilience appears explicitly in core capabilities under the mitigation mission, one of the more recently added homeland security missions that is actually an outcome of the other missions being successful.[76]

- *Community Resilience* seeks to provide the ability to behave resiliently across all the phases of a given threat or hazard—to resist, absorb an impact, degrade gracefully if necessary but maintain critical functions, respond effectively and remain a short time in that position, and recover full performance rapidly.[77]
- *Long-term Vulnerability Reduction* aims at lessening the likelihood, severity, and duration of adverse consequences related to these adverse incidents. Such outcomes can be obtained in part by incorporating appropriate resilience core capabilities of communities, critical infrastructures, and key resources.
- *Risk and Disaster Resilience Assessment* entails assessment of risk and disaster resilience so that decision makers, responders, and community members can take informed, specific actions to reduce their entity's risk and increase their resilience.

To wrap up this discussion, the DHS Strategic Plan for FY2012 -16 rests upon the five *QHSR* missions, with resilience tied to the mission of disaster relief, but also connected in an operational sense to making critical infrastructure resilient to both traditional and cyber threats.[78]

Tactical Initiatives

Resilience has continued to influence a series of initiatives at what might be called the "tactical level" – not emphasizing strategic concepts, but working from the bottom up "by taking important steps to help our state and local partners strengthen the resilience of their infrastructure, computer networks, and of their communities and citizens."[79] A number of steps have been taken towards meeting these rather expansive goals.

Item: DHS Definition of Resilience. The Resilience Integration Team (RIT), formed by The Office of Resilience Policy (ORP), seeks to provide component DHS agencies with a single, consistent, department-wide understanding of resilience and helps components understand how their activities address DHS's proposed resilience objectives.[80] ORP officials appear to have failed thus far in even producing an approved generalized policy statement, given the less then cooperative reactions from the components across the Department.[81]

Item: Resilience STAR™. The Resilience *STAR™* Home Pilot Project, modeled after the existing Energy STAR Program, entails DHS working with homeowners and builders to assist in designing or remodeling structures with features that can enhance their resilience to high consequence natural disasters they are facing. It is unclear how successful this initiative will turn out to be, as many economic and socio-political challenges need to be overcome. However, this initiative has at least been given visibility in Congress.[82]

Item: Regional Infrastructure Resilience. *Presidential Policy Directive (PPD)-21* calls for advancing national unity through strengthening and maintaining secure, functioning, and resilient critical infrastructure.[83] The Regional Resiliency Assessment Program (RRAP) is an interagency assessment of a specified set of U.S. critical infrastructure and key assets, combined with a regional analysis of the surrounding infrastructure, including key interdependencies. RRAP evaluates critical infrastructure "clusters," regions, and systems to reduce the nation's vulnerability to all-hazard threats by coordinating efforts to enhance CI/KR resiliency and security across geographic regions.[84]

Item: Incentivize private businesses. DHS is leading in an interagency effort to provide voluntary incentives for small and large businesses to take steps that enhance their resilience. The case is being made that improved resilience can enhance the success of private businesses. Guidelines are being set for estimating private sector preparedness and identifying needed improvements.[85]

Item: New Technologies. The DHS Science and Technology Directorate (S&T) has been developing new technologies, models, and other tools that promote resilience. A summit of experts hosted by the S&T Office of University Programs addressed how science and technology can "contribute to shaping our resiliency blueprint by instilling scientific rigor into the processes that will shape our future, [...and] how can the nation's operational resilience be improved?"[86]

Item: Campus Resilience Pilot Program. Under the Campus Resilience Pilot Program (CR Pilot) DHS works with seven selected colleges and universities "to draw on existing resources, collaborate with federal, state and local stakeholders and identify new innovative approaches to promote campus resilience."[87]

Item: Human Resilience. The *Together* Employee and Organizational Resilience Program was developed to enhance the health and well-being of all DHS employees. The program is bringing together employees from across the Department, managers as well as staff, to discuss best practices and creative concepts for identifying resilience issues.[88]

It remains to be seen how effective these initiatives will turn out to be or whether others may be launched.

CONCLUSION

While the basic idea of resilience seems relatively straightforward, upon closer scrutiny this question of credibly and effectively operationalizing resilience across the nation at all public and private levels is inherently complex. The fact that we see resilience appearing on the level of homeland security missions, as discussed earlier, is clearly a step forward.

What we do not see, however, are analytic guideposts on how to plan and execute the establishment of concrete resilience programs for all classes of important systems that might experience specified adverse events across all domains for all levels of stakeholders. Also missing are guidelines for how to measure needs or gaps in resilience and progress achieved after steps are taken. There are challenges in defining, assessing, and integrating threats, targets, and risks, as well as uncertainties in understanding and analyzing large numbers of interrelated elements. Policy, resource, and other constraints also need to be considered. In terms of bringing analytic capabilities to bear, a group of experts argues that a "systems approach" can help in analyzing the nature of resilience, which " entails viewing systems as complex networks with dynamic behavior and many interdependencies that could be exploited by adversaries."[89] Such complex networks tend to be difficult to understand and analyze, with outcomes that are either non-existent or virtually impossible to understand.[90]

Without concerns over analytic complexity or even meanings and measurements, resilience might well continue to be used in simple ways to prepare a community or business to deal with different threats and hazards, as in the tactical applications of resilience by DHS, such as those listed earlier. Furthermore, the world of academia will almost certainly continue to address the issue of resilience through writings to be published, courses to be taught, and conferences to attend. Looked at another way, if resilience is to be a leading homeland security concept, advocates might see that "achieving resilience is not a destination, but a journey on which we must lead all citizens."[91] Presumably, "we" stands, not only for DHS and other federal agencies, but also state and local governments, communities, and the academic and research fields.

This article explored homeland security through the lens of resilience. However, upon completion of the material in this article, the author has reached what may seem like an odd conclusion. He would ask readers to appreciate the idea that *too much of a focus on operationalizing resilience would have the effect of putting the resilience cart before the preparedness horse*. This means that *PPD-8* implementation, at the moment, is leading the way in trying to improve national preparedness from the bottom–up as well as from the top-down.[92] If *PPD-8* implementation progresses and nationwide as well as regional and local preparedness improves, the resilience of individuals, communities, businesses, NGOs, and all levels of government will *perforce* tend to increase. Given the analytical and governance challenges *PPD-8* implementation faces, however, if this initiative fails to improve preparedness across the nation at all levels, these resilience benefits will not emerge.

Whatever the future of *PPD-8*, homeland security policies and programs, the author would agree that issues of defining and measuring resilience will almost certainly remain an active topic. Resilience *mavens,* be of good cheer. This term will remain resilient for a long time, although not competing with the cockroach: a species that has been on earth for over 350 million years, known for its hardiness and ability to survive in the most demanding situations, even nuclear war.[93]

About the Author

Jerome Kahan *is currently an independent writer and analyst. He was formerly a Distinguished Analyst at the Homeland Security Studies and Analysis Institute in Arlington, VA. Mr. Kahan has been in the national security, arms control, and homeland security fields for over 40 years—including 20 years with the Department of State, where he held positions on the Policy Planning Staff and as Deputy Assistant Secretary with the Political-Military and Intelligence Bureaus and served as Counselor at the American Embassy in Turkey. He worked for many years with non-governmental research organizations, including the Brookings Institution, the Center for Naval Analyses, and Systems Planning and Analysis. He has written and/or contributed to a number of books, published articles in a variety of journals, taught at the Air Force Academy, and served as an Adjunct Professor in the School of Foreign Service at Georgetown University. He has also been a member of the Council on Foreign Relations and the International Institute of Strategic Studies. Mr. Kahan holds a Masters Degree in Electrical Engineering from Columbia University, with Bachelor's Degrees from Queens as well as Columbia College. Jerome Kahan can be reached at jhkahan@cox.net.*

Notes

1. Resilience' originated in the 16th and 17th centuries, deriving from the verb 'resile,' which in turn was drawn from the Latin verb 'resilire,' meaning to 'jump back, recoil.' [For centuries…] "resilience enjoyed a broad kind of usage, referring loosely both to a property of physical matter (such as elastic or springing objects) and to personal characteristics (such as tending to recover quickly or easily from misfortune, shock, illness, or the like; buoyant, irrepressible; adaptable, robust, hardy)." Sam Gardner, et al., *Resilience in Eight Key Questions and Answers,* Reaching IN…Reaching OUT (RIRO), Toronto CA, 2. http://www.reachinginreachingout.com/documents/MCYSResilienceReport11-16-10Dissemination.pdf.

2. For example, in 1986 the National Science Foundation established a national center for earthquake research that in 1998 became the Multinational Center for Earthquake Engineering Research (MCEER), Headquartered at the University at Buffalo. http://mceer.buffalo.edu/.

3. One such organization is the Community and Resilience Institute (CARRI) for helping communities strengthen their ability to withstand and recover from adverse incidents. See *Community & Regional Resilience Institute*. resilientus.org**.** Other organizations include The Resiliency Center in Portland, Oregon and The Torrance Resilience Institute in Adelaide, Australia.

4. T*he National Commission on Terrorist Attacks Upon the United States* (also known as the *9-11 Commission*), was an independent, bipartisan commission created in late 2002 "chartered to prepare a full and complete account of the circumstances surrounding the September 11, 2001 terrorist attacks, including preparedness for and the immediate response to the attacks." www.911commission.gov/report/911Report.pdf.

5. U.S. Department of Homeland Security*, Quadrennial Homeland Security Review* (QHSR) February 2010, June 2014; Washington. DC.

6. Executive Office of the President, Presidential Policy Directive-8 (PPD8), February 2011, Washington, DC, 6.

7. In this sense, the parable of the *Blind Men and the Elephant* comes to mind. In the story, as different blind men touch different parts of an elephant, each reaches a different conclusion about what they were touching—a tree for each leg, a hose for the tail, spears for the tusks, and so on. To illustrate this point, the author published a poem designed to show that resilience as applied to homeland security is indeed like the elephant in this parable. Jerome H. Kahan, *Understanding Resilience: The Blind Men and the Elephant***,** Journal of Homeland Security Education, Volume 2 (2013).

8. Jerome H. Kahan, "What's in a name? The meaning of homeland security," *Journal of Homeland Security Education 2, (January 2013),* 1-18. At http://www.journalhse.org/v2jeromekahan.html.

9. The academic literature is replete with articles not only by U.S. authors but also by experts from Australia, Israel, and other foreign nations.

10. Active resistance before impact includes pre-event efforts to thwart, attenuate, or redirect the threat/hazard/disruption before it impacts. See Jerome H. Kahan, et al., "Operational Framework for Resilience*," Journal of Homeland Security and Emergency Management* 6, no.1 (2009). http://dx.doi.org/10.2202/1547-7355.1675.

11. Homeland Security Advisory Council, *Community Resilience Task Force Report,* Department of Homeland Security, Washington, DC, June 2011.

12. An analytic basis for this relationship can be found in Jerome Kahan, et al., *Risk and Resilience: Exploring the Relationship,* Homeland Security Studies and Analysis Institute, Department of Homeland Security, (Washington, DC), November 22, 2010. This was done for the DHS Science and Technology Directorate, but does not necessarily reflect official DHS opinion or policy. As stated in the preface, "The purpose of this task is to define and measure resilience in practical terms, and to examine the relationship between risk and resilience in the homeland security context, with potential value for policy makers and planners". The report was approved for public release.

13. Patrick Martin-Breen and J. Marty Anderies, *Resilience: A Literature Review,* Sponsored by Rockefeller Foundation, September 18, 2011. Examples of articles that deal with unusual applications of resilience, such as resilience applied to ecosystems, include Brian Walker and David Salt, *Resilience Thinking: Sustaining Ecosystems and People in a Changing World* (Washington, DC: Island Press, 2006).

14. Kathleen Tierney and Michel Bruneau, "Conceptualizing and Measuring Resilience," *TR News* 250*,* May-June 2007, 14-17. David Arsenault and Arun Sood, "Measuring Resilience in Network-Based Infrastructures," from *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, George Mason University School of Law, Critical Infrastructure Protection Program, 2007, 87-95.

15. This construct is based on the approach taken in the HSSAI report already cited, but adds the additional domain of individuals to the four domains used in that effort. See Kahan, *Risk and Resilience,* 7-110.

16. R*esilience* has been applied for decades in assessing the way individuals behave in stressful situations. Torrens Resilience Institute, *Resilience* of *Individuals, Australia,* http://www.torrensresilience.org/resilience-of-individuals.

17. Groundbreaking work on infrastructure resilience was done in 2005 by Stephen Flynn in *America the Vulnerable: How Our Government is Failing to Protect Us from Terrorism* (Council on Foreign Relations Press: New York, NY).

18. Economists have made the argument that investments in high resilience programs in a competitive market help maintain continuity of operations in the event of emergencies and can therefore offer potentially cost effective competitive advantages. For resilience in the business context see Yossi Sheffi, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage* (Cambridge, MA: The MIT Press, 2005).

19. While less obvious a domain of interest to the homeland security enterprise than the other domains, ecosystems can affect the nation's food and fuel supply, the environment, and overall quality of life. When responding to disruptions, an ecosystem seeks to maintain existence of its fundamental function, if necessary by "flipping" into one of a number of possible different states within its "regime of behavior" and avoiding moving into a fundamentally and qualitatively different state, C.S. Holling, "Article 3- The Resilience of Terrestrial Ecosystems," in Lance Gunderson et al., *Foundations of Ecological Resilience* (Island Press: Washington, 2010).

20. For an elaboration on this concept and other indicators of community resilience, see Cutter, et al., "Disaster Resilience Indicators for Benchmarking Baseline Conditions," *Journal of Homeland Security and Emergency Management* 7, no.1, article 51, (2010), 6-9. An expert argued, "Even with unlimited resources, it is highly unlikely that a community can prevent or protect itself from all the possible dangers it may face. The greater the uncertainty, the greater the need for flexibility. Yet, the pervasiveness of "worst-case," "probabilistic" planning lacks the "possibilistic thinking" needed to face both the dangers *and* the opportunities that no one can predict….," Patricia H. Longstaff, et al., "Building Resilient Communities: A Preliminary Framework for Assessment," *Homeland Security Affairs* 6, no.3, September 2010. http://www.hsaj.org/?article=6.3.6.

21. Consider the argument that "the definition of resilience "should be independent of the object of analysis …in the interest of facilitating the formulation of compatible policy goals in both the public and private sectors by a range of actors…the same definition should be used in all decision-making processes. Establishing a uniform definition is critically important… will affect how we distinguish between resilience and other measures – specifically, protection and vulnerability – of our ability to withstand the adverse effects of natural and man-made threats." L. Carlson et al., *Resilience Theory and Applications*, Argonne National Laboratory, Decision and Information Sciences Division, (Oak Ridge, TN, January 2012). reports@adonis.osti.gov.

22. A planning technique called "snake diagrams" is employed to visually assist users in making the appropriate choice. See Kahan, et al., *Risk and Resilience.*

23. This particular definition of resilience is taken from the Governor's Office of Homeland Security & Emergency Preparedness, State of Louisiana Strategic Plan, (July 2010).

24. Adam Rose, "Economic Resilience to Natural and Man-made Disasters: Multidisciplinary Origins and Contextual Dimensions," *Environmental Hazards 7,* no.4*, (*2007), 383-398. http://www.tandfonline.com/doi/abs/10.1016/j.envhaz.2007.10.001#.VMh3g2jF-ZM.

25. See A. McCarthy, "Introduction: From Protection to Resilience: Injecting "Moxie" into the Infrastructure Security Continuum," C*ritical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, George Mason University School of Law Critical Infrastructure Protection Program, 2007, pp. 1-7. See also Stephen Flynn, *The Edge of Disaster* (New York: Random House, 2007), 154; and Stephen Flynn, "America the Resilient," *Foreign Affairs* 87, no. 2 (March/April 2008), 7.

26. National Infrastructure Advisory Council, *Framework for Establishing Critical Infrastructure Resilience Goals, Final Report and Recommendations by the Council.* Introduction, October 19, 2010. The National Infrastructure Advisory Council (NIAC) provides the President of the United States with advice on the security and resilience of the

critical infrastructure sectors and their functional systems, physical assets, and cyber networks. www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

27. National Infrastructure Advisory Council, *Strengthening Regional Resilience through National, Regional, and Sector Partnerships,* Draft Report and Recommendations, November 21, 2013.

28. The National Infrastructure Protection Plan (NIPP) entitled *NIPP 2013*: *Partnering for Critical Infrastructure Security and Resilience* outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes. NIPP 2013 meets the requirements of *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*, signed in February 2013. *National Infrastructure Protection Plan*. http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

29. Community resilience pilot projects have been organized by such groups as the Red Cross. See American Red Cross *Community Resilience Pilot* Program http://www.rwjf.org/en/blogs/new-public-health/2012/02/preparedness-summit-american-red-cross-community-resilience-pilot-program.html; Also states and cities have sponsored community resilience projects, such as City of Alexandria *Community Resiliency* Program, and the *New Jersey Coastal Resiliency Enhancement Project 1*. Finally, there is the specialized resiliency-skills training program in private practice and in the community. RIRO Resiliency Guidebook - Reaching IN…Reaching OUT http://www.reachinginreachingout.com/documents/Guidebook-06.pdf.

30. Homeland Security Advisory Council, *Community Resilience Task Force Report,* (Washington, DC, June 2011).

31. Preparedness, Response, and Resilience Task Force, *Operationalizing Resilience,* the George Washington University Homeland Security Policy Institute, (Washington, DC October 13, 2011).

32. Ibid. Exactly what is meant by a "systems approach" for use by communities desiring to set and reach resilience goals is not developed.

33. National Research Council, *Disaster Resilience: A National Imperative*, (Washington, DC: The National Academies Press, 2012).

34. See Jerome H. Kahan et al., *"*An Operational Framework for Resilience*," Journal of Homeland Security and Emergency Management* 6, no. 1, 2009. http://dx.doi.org/10.2202/1547-7355.1675.

35. Ibid. Also the *Risk and Resilience* effort by *HSSAI* offers a "Resilience Profile" model for measuring and comparing the resilience of different systems—simplifying the so-called "bathtub" shape that describes a system's behavior after experiencing a disruption. The degree of resilience is measured by the total area within the resilience profile using metrics of performance-time units. The larger the area bounded by the profile of a particular system, the less resilient it is to a given threat or hazard. Planners can use the shape of a profile to compare and contrast different ways a system might be made resilient. Bathtub curves depicting a system's performance after being impacted by adverse events appear in many sources, including Yossi Sheffi, *The Resilient Enterprise*, 65; and Mary Ellen Hynes, "Extreme Loading of Physical Infrastructure," presentation given at the 4th DHS University Network Summit, (Washington DC, March 11, 2010).

36. David Arsenault and Arun Sood, "Measuring Resilience in Network-Based Infrastructures", 87-95. For example, if a circuit breaker is too resilient to a large power surge, it may resist shutting down power, with major consequences to the system.

37. "Measure" is any characteristic of a real system (e.g. quality, dimension, or behavior) that can describe or explain how or why it is resilient. The key is to find measurements of *effectiveness,* not measures of *performance*. *Metrics* are needed to give a more specific, preferably quantitative, output on the scope, scale, strength, or duration of a given measure.

38. General Accounting Office, *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency are Evolving but Program Management Could be Strengthened, An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure*, GAO-10-777, (Washington D.C., October 2012), 32-34.

39. Ibid.

40. For example, a method developed by the DHS Science & Technology (S&T) Resilient Systems Division (RSD) provides a framework for identifying resilience of a wide range of facilities based on a multi-hazard approach that incorporates interactions between facility characteristics. The results provide both a baseline for establishing relative resilience, as well as an indication of deficiencies and a path to their mitigation. Presented on January 6-11, 2014 at the National Institute of Building Science Integrated Resilient Design (IRD) Symposium on Measuring and Improving Resilience of Existing Facilities. Building Innovation 2014 Conference & ExpProgram:IRD **...** www.nibs.org/?page=conference14_ird.

41. Kahan et al., *Risk and Resilience.*

42. Community Resilience Task Force (CRTF) 34, Recommendation 3.4: "*Enable Community-Based Resilience Assessment*. DHS should coordinate development of a community-based, all-hazards American Resilience Assessment (ARA) methodology and toolkit."

43. The *HSSAI, f*or example, developed a relatively simple method for the Department to consider as an initial step in the direction of providing communities with a qualitative approach for assessing their resilience. See Jerome H, Kahan, et al., *Community Resilience Profiles: Assessment and Evaluation, HSSAI Report, p*repared for Department of Homeland Security, Science and Technology Directorate, December 19, 2011, Cleared for public release.

44. A comprehensive study by Argonne National Laboratory in 2012 argues, "The resilience of a community/region is a function of the resilience of its subsystems, including its critical infrastructures, economy, civil society, governance (including emergency services), and supply chains/dependencies…As we move to the community/regional level, the assessment of the resilience becomes a much more complex task that involves investigation of the resilience of numerous aspects of the community or region, including the local economy, critical infrastructure, civil society, governance (including emergency services), and supply chains. The number and complexity of these subsystems will make the measurement of resilience more challenging as we move from individual assets/facilities to the community/regional level (where critical infrastructure resilience is only one component)." L. Carlson et al., *Resilience: Theory and Applications*, Argonne National Laboratory, Decision and Information Sciences Division, (Oak Ridge, TN: January 2012). reports@adonis.osti.gov.

45. Patricia H. Longstaff et al., "Building Resilient Communities: A Preliminary Framework for Assessment," *Homeland Security Affairs* 6, no. 3, (September 2010). http://www.hsaj.org/?article=6.3.6.

46. President Barack Obama, A Proclamation: National Preparedness Month, 2009, Office of the Press Secretary, (Washington DC, September 4, 2009).

47. President G.W. Bush, *Address to the Nation on the Terrorist Attacks,* September 11, 2001.

48. "President Bush Announces Office of Homeland Security," September 20, 2001, POLITICO.

49. *National Strategy for Homeland Security,* Office of Homeland Security, The White House (Washington DC, 2002).

50. Congressional Research Service, *Federal Emergency Management Policy Changes After Hurricane Katrina: A Summary of Statutory Provisions*, CRS Report for Congress, (Washington, DC, November 15, 2005), 20.

51. *National Strategy for Homeland Security,* Homeland Security Council, The White House (Washington DC, 2007).

52. Department of Homeland Security, *One Team, One Mission, Securing Our Homeland,* U.S. Department of Homeland Security Strategic Plan: Fiscal Years 2008–2013, February 2008. The first Strategic Plan, FY 2004- 8, did not include resilience as a vision, goal, or objective.

53. "Resilience Blooming Into Its Own," *Homeland Security Watch,* May 1, 2008. Also, see "Committee Leaders Pleased with Month of Hearings on Resiliency," *CQ Homeland Security,* May 23, 2008.

54. *The National Security Strategy of the United States of America,* The White House, (Washington DC, June 2010), 18.

55. QHSR 2010, 15. *The Bottom Up Review (BUR),* issued shortly after the first QHSR, reiterated that, "despite our best efforts, some attacks, accidents, and disasters will occur. Therefore, the challenge is to foster a society that is robust, adaptable, and has the capacity for rapid recovery. In this context, individuals, families, and communities—and the systems that sustain them—must be informed, trained, and materially and psychologically prepared to withstand

disruption, absorb or tolerate disturbance, know their role in a crisis, adapt to changing conditions, and grow stronger over time." Bottom-Up Review Report, (Washington, DC, July 2010), Executive Summary.

56. First QHSR, 2010, 14.

57. Ibid., 14-16.

58. Barack Obama, *Presidential Policy Directive/PPD-8,* (Washington, DC) March 30, 2011.

59. NPG, 1.

60. Barack Obama, *Presidential Policy Directive 21-- Critical Infrastructure Security and Resilience,* The White House, Washington, DC, (February 12, 2013).

61. Barack Obama, *Executive Order, 13636, Improving Critical Infrastructure Cybersecurity,* The White House, Washington, DC, (February 12, 2013).

62. QHSR, 2014, 58.

63. Ibid., 72.

64. Ibid., 74.

65. Ibid., 24.

66. FY 2008 DHS Strategic Plan: Objective 3.1.

67. See Kahan, *Operational Framework*.

68. Preparedness, Response, and Resilience Task Force, "Operationalizing Resilience," Homeland Security Policy Institute, the George Washington University, Oct 13, 2011.

69. Brandon Wales, Director, DHS Threat and Risk Analysis Center, at panel held by the Center for National Policy, reported by Jennifer Scholtes, *Congressional Quarterly*, Washington, DC, January 12, 2011.

70. GAO, 2012.

71. QHSR, 2010, 20.

72. The mission is "Create a Safe, Secure, and Resilient Cyber Environment," *QHSR,* 2010, 30.

73. The author is currently preparing an article comparing the two QHSRs.

74. Recall the author's meaning of "behaving resiliently" in the earlier section on definitions.

75. The following points are closely drawn from the document in question.

76. Prior to the first QHSR, the four official homeland security missions did *not* include mitigate. This was added later, likely due to FEMA's advocacy. Mitigation is not actually a frontline mission. The NPG says this mission derives from the successful operation of the four other missions. If there is mitigation on the ground, the NPG states that "individuals, the private sector, communities, critical infrastructure, and the nation as a whole are made more resilient when the consequences and impacts, the duration, and the financial and human costs to respond to and recover from adverse incidents are all reduced." NPG, 9.

77. See Kahan et al., *Community Resilience Profiles: A Diagnostic Approach,* Homeland Security Studies and Analysis Institute, conducted for the Department of Homeland Security Science and Technology Directorate, 2009. Cleared for public release.

78. Department of Homeland Security, *The U.S. Department of Homeland Security Strategic Plan for Fiscal Years 2012-2016* Washington, DC, (February 2012).

79. *Rebuilding the Foundation for America's Home Security*, Remarks prepared by Secretary Napolitano to New York City First Responders, New York City Emergency Operations Center, released September 10, 2010.

80. General Accounting Office, *An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure*, GAO-13-11 Washington, DC, (Oct 25, 2011). www.gao.gov/products.

81. GAO auditors observed, "a strategy that establishes organizational responsibilities and a coordination mechanism, identifies performance measures, and traces funding sources would likely improve overall resilience efforts and provide ORP with a more complete picture of how DHS components are implementing this policy." GAO, 2012. A 2010 survey by the DHS Office of Policy found that component resilience actions were stove-piped and proposals for integrating resilience referred to as "'works in progress."

82. Mike Kangior and Matt Fuchs, *Engineering Resilience, Home Pilot Project,* November 16, 2013, DHS Office of Policy, At *Engineering Resilience*: The Resilience STAR™ *Home Pilot Project* http://www.dhs.gov/blog/2013/11/18/engineering-resilience-resilience-star%E2%84%A2-home-pilot-project Appearing before Congress, an insurance firm official recommended prioritizing investments in resilience over funding for disaster response, stating "Currently in the United States, many privately and publicly held assets, from homes to critical infrastructure, are not sufficiently 'resilient' to withstand extreme weather events…From a practical perspective, funding resilience is a fundamentally wiser investment than spending on disaster relief and recovery," One way to do so… would be to expand a Homeland Security Department pilot project called Resilience Star that's based on the same logic as Energy Star certification." L. Patton. Zurich Insurance, Statement before Senate Homeland Security and Governmental Affairs Committee, February 12, 2014. www.hsgac.senate.gov.

83. Barack Obama, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience,* February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

84. Homeland Security *Regional Resiliency Assessment Program (RRAP).* http://www.dhs.gov/regional-resiliency-assessment-program.

85. This is aimed at facilitating greater acknowledgement of preparedness by the insurance industry, rating agencies, legal community, supply chain management arena, and others. William Raisch, "A Missing Link between Business Resilience & Incentives?" *A New U.S. Law and Corporate Preparedness*, Director of the International Center for Enterprise Preparedness (Inter CEP), 2007. http://www.nyu.edu/intercep/A%20Missing%20Link%20Between%20Business%20Resilience%20%26%20Incentives.htm.

86. Dr. Mitchell Erickson, *Science and Technology at DHS: Resiliency of our Physical and Social Infrastructure,* Department of Homeland Security, April 11, 2012. At this conference it was decided to adopt the theme of "intelligent resilience—how to maximize minimal resources."

87. The CR Pilot was created in 2013 upon recommendation from the DHS Homeland Security Academic Advisory Council (HSAC) comprised of prominent university presidents and academic leaders, and charged with advising the Secretary and senior leadership at the Department on matters related to homeland security and the academic community, including campus resilience.

88. *Together* Program, Department of Homeland Security.

89. *Resilience: Theory and Applications,* Executive Summary.

90. For a discussion of why homeland security solutions represent so-called wicked problems, see Jay Rosen, "What Are Journalists For?" PressThink.org, 2005. Also see James Jay Carafano and Richard Weitz, *Complex Systems Analysis-A Necessary Tool for Homeland Security,* Heritage Foundation, Backgrounder #2261, April 16, 2009.

91. HSPI Task Force Report, 2-4.

92. See Jerome H. Kahan, "Preparedness Revisited: W (h)ither *PPD-8*?." *Homeland Security Affairs* 10, article 2 (February 2014). http://www.hsaj.org/?article=10.1.2.

93. "The Immortal *Cockroach," Global Times*, February 20, 2013. http://www.globaltimes.cn/content/763012.shtml.